ROURKELA SMART CITY LIMITED

RFP. No. RSCL/110/2018/352

Request for Proposal for Selection of Master System Integrator (MSI) for Implementation of Smart Solutions in Rourkela

Volume 2

Scope of Work

Date: 25 July 2018

----------This Page is intentionally left blank----------

Disclaimer

The information contained in this Request for Proposal document ("RFP document") or subsequently provided to Applicant(s), whether verbally or in writing or in any other form, by or on behalf of Rourkela Smart City Limited. (hereafter referred to as "RSCL") or any of its employees or advisors, is provided to the Applicant(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided in writing.

This RFP document is intended to be and is hereby issued only to the prospective Applicants. The purpose of this RFP document is to provide the Applicant(s) with information to assist the formulation of their Proposals. This RFP document does not purport to contain all the information that each Applicant may require. This RFP document may not be appropriate for all persons, and it is not possible for the RSCL, its employees or advisors to consider the investment objectives, financial situation and particular needs of each applicant who reads or uses this RFP document. The assumptions, assessments, statements and information contained in the RFP document may not be complete, accurate, adequate or correct. Each Applicant should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP document and where necessary obtain independent advice from appropriate sources. The RSCL, its employees and advisors make no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, adequacy, correctness, reliability or completeness of the RFP document.

Information provided in this RFP document to the Applicant(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement in law. RSCL accepts no responsibility for the accuracy or otherwise for any interpretation or opinion expressed herein.

RSCL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any applicant under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP document or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP document and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP document or arising in any way for participation.

RSCL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Applicant upon the statements contained in this RFP document.

RSCL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP document before the last date of bid submission. RSCL also may in its absolute discretion cancel the entire RFP, without providing any reason.

The issue of this RFP document does not imply that RSCL is bound to select an Applicant or to appoint the selected Applicant or Master System Integrator, as the case may be, for the Project and the RSCL reserves the right to reject all or any of the Applicants or Bids without assigning any reason whatsoever.

The Applicant shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by the RSCL or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Applicant and the RSCL shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an Applicant in preparation or submission of the Bid, regardless of the conduct or outcome of the Bidding Process.

----------This Page is intentionally left blank----------

Table of Contents

Abbreviations

Acronym	Definition
AAA	Authentication, Authorization, and Accounting
AAC	Augmentative and Alternative Communication
ABC	Activity Based Costing
ABD	Area Based Development
ACD	Automatic Call Distributor
ACL	Access Control List
ADC	Application Delivery Controller
ADS	Active Directory Services
AES	Advanced Encryption Standard
AFIS	Automatic fingerprint identification system
AGC	Automatic Gain Control
AHU	Air Handling Units
AIX	Advanced Interactive eXecutive
AJAX	Asynchronous JavaScript and XML
AMD	Advanced Micro Devices
AMQP	Advanced Message Queuing Protocol
ANI	Automatic Number Identification
ANPR	Automatic Number Plate Recognition
ANSI	American National Standards Institute
APFC	Active Power Factor Correction
API	Application Program Interface
APP	Application
ARP	Address Resolution Protocol
ARV	After Repaired Value
ASC	Auto Signal Compensation
ASCE	American Society of Civil Engineers
ASCII	American Standard Code for Information Interchange
ASI	Archaeology Survey Of India
ASR	Automated Speech Recognition
ASTM	American Society for Testing and Materials
ATC	Adaptive Traffic Control
ATCS	Adaptive Traffic Control System
ATM	Automatic Teller Machine
ATP	Acceptance Test Procedures
AVC	Advance Video Coding
AVI	Audio Video Interleave
AWS	Amazon Web Services
BEE	Bureau of Energy Efficiency
BGP	Border Gateway Protocol
BHIM	Bharat Interface for Money
BIOS	Basic Input / Output System
BIS	Bureau Of Indian Standard
BLC	Back Light Compensation
BMP	Bitmap
BMS	Building Management System
BOQ	Bill of Quantities
BOT	Build Operate Transfer

Acronym	Definition
BPAS	Building Plan Approval System
BPEL	Business Process Execution Language
BPM	Business Process Management
BPMN	Business Process Modeling Notation
BPR	Business Process Reengineering
BPUT	Biju Patnaik University of Technology
BSI	British Standard Institution
BSNL	Bharat Sanchar Nigam Ltd.
BSSID	Basic Service Set Identification
BTU	British Thermal Unit
BYOD	Bring Your Own Device
CAD	Computer Aided Design
CAF	Common Application Form
CAGR	Compound Annual Growth Rate
CAN	Controller Area Network
CBC	Cell Broadcast
CBEFF	Common Biometric Exchange Formats Framework
CBR	Constant Bit-Rate
CBS	Cell Broadcasting Service
CBT	Computer Based Training
CCC	Command and Control Centre
CCD	Charge Coupled Device
CCTV	Closed Circuit Television
CDAC	Centre for Development of Advanced Computing
CDMA	Code Division Multiple Access
CDRW	Compact Disc-ReWritable
CEF	Common Event Format
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CFC	Citizen Facilitation Centre
CIE	Control and Indicating Equipment
CIF	Common Intermediate Format
CIFS	Common Internet File System
CIP	Construction In Progress
CIS	Computer Information System
CLI	Caller line identification
CMDB	Configuration Management Database
CMGI	Center for Modernizing Government Initiative
CMOS	Complementary Metal-Oxide Semiconductor
CMS	Content Management System
CNTK	Cognitive Toolkit
COTS	Commercial Off The Shelf
CPC	Common Payment Card
CPCB	Central Pollution Control Board
CPE	Customer Premises Equipment
CPF	Central Provident Fund
CPU	Central Processing Unit
CQL	Common Query Language
CRC	Cluster Resource Coordinators

Acronym	Definition
CRCA	Cold Rolled Close Annealed
CSP	Cloud Service Provider
CSS	Cascading Style Sheets
CSV	Comma Separated Values
CTI	Computer Telephony Integration
DARPG	Department of Administrative Reforms and Public Grievances
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DCMS	Display Content Management System
DCS	Distributed Control System
DDC	Digital Direct Controller
DDE	Dynamic Data Exchange
DDOS	Distributed Denial of Service
DDS	Digital Display Screen
DHCP	Dynamic Host Configuration Protocol
DIL	Dual in Line
DIMM	Dual In-line Memory Module
DIT	Department of Information Technology
DIY	Do It Yourself
DLCI	Data Link Connection Identifier
DLL	Dynamic Link Library
DNIS	Dialled Number Identification Service
DNR	Digital Noise Reduction
DNS	Domain Name Service
DOB	Date of Birth
DOD	Date of Death
DOT	Department of Telecom
DPI	Dots per Inch
DPS	Delhi Public School
DRAM	Dynamic Random Access Memory
DRC	Disaster Recovery Centre
DSC	Digital Signature Certificates
DSCP	Differentiated Services Code Point
DSP	Digital Signal Processor
DSS	Data Security Standard
DTMF	Dual-Tone Multi-Frequency
DTV	Digital Television
DVD	Digital Video Disc
DVI	Digital Visual Interface
DVMRP	Distance Vector Multicast Routing Protocol
DWG	AutoCAD drawings
EAI	Enterprise Application Integration
EAP	Extensible Authentication Protocol
ECB	Emergency Call Button
ECC	Error-correcting code
ECM	Enterprise Content Management
ECMP	Equal Cost Multi Path
EDGE	Enhanced Data for GSM Evolution
EDR	Enhanced Data Rate

Acronym	Definition
EGIF	e-Government Interoperability Framework
EIA	Electronic Industries Alliance
EIRP	Effective Isotropic Radiated Power
EMD	Earnest Money Deposit
EMS	Environment Monitoring System
EMV	Europay, MasterCard, Visa
EOI	Expression of Interest
EPABX	Electronic Private Automatic Branch Exchange
EPC	Evolved Packet Core
ERP	Enterprise Resource Planning
ESB	Enterprise Service Bus
ESQL	Extended Structured Query Language
ETSI	European Telecommunications Standards Institute
EWS	Economically Weaker Section
FAQ	Frequently Asked Questions
FAR	Floor area ratio
FAT	Factory Acceptance Test
FATCS	Full adaptive traffic control system
FCC	File Client Cache
FCR	Field Call Report
FCU	Fan Coil Units
FIFO	First-In First-Out
FIPS	Federal Information Processing Standardisation
FOB	Free On Board
FPE	Format Preserving Encryption
FPS	Frames Per Second
FRS	Facial Recognition System
FTP	File Transfer Protocol
GAAP	Generally Accepted Accounting Principles
GBPS	Gigabits Per Second
GCP	Garbage Collection Point
GCSS	Gateway Common Services Specifications
GDPR	General Data Protection Regulation
GHZ	Gigahertz
GIF	Graphics Interchange Format
GIGW	Guidelines for Indian Government Websites
GIS	Geographic Information System
GML	Geography Markup Language
GOI	Government of India
GPRS	General Packet Radio Service
GPS	Global Positioning System
GPU	Graphics Processing Unit
GRC	Governance, Risk management, and Compliance
GRV	Goods Received Voucher
GSM	Global System for Mobile Communications
GST	Goods and Service Tax
GUI	Graphical User Interface
HBA	Host Bus Adapter
HDCP	High Definition Copy Protocol

Acronym	Definition
HDD	Hard Disk Drive
HDMI	High Definition Multimedia Interface
HDTV	High Definition Television
HFE	Human Factors Engineering
HRM	Human Resource Management
HRMS	Human Resource Management System
HSD	High Speed Diesel
HTML	Hypertext markup language
HTTP	Hypertext transfer protocol
HTTPS	Hypertext transfer protocol secure
HVAC	Heating Ventilation and Air Conditioning
ICCC	Integrated Command and Control Centre
ICDS	Integrated Child Development Services
ICES	Interference-Causing Equipment Standard
ICIIPC	National Critical information Infrastructure Protection Centre
ICMP	Internet Control Message Protocol
ICT	Information & Communication Technologies
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFEG	Interoperability Framework for e-Governance
IGH	Ispat General Hospital
IGIS	Inter-Gateway Interconnect Specifications
IIP	Interoperability Interface Protocol
IIS	Interoperability Interface Specifications
ILFS	Infrastructure Leasing and Financial Services
ILT	Instructor-Led Training
IMAP	Internet Message Access Protocol
IMP	Immediate Mobile Payment
IMPS	Immediate Mobile Payment System
INR	Indian Rupee
IOS	iPhone Operating System
IOT	Internet of Things
IPFIX	Internet Protocol Flow Information Export
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISI	Indian Standards Institute
ISSU	In Service Software Upgrade
ITIL	Information Technology Infrastructure Library
ITMS	Intelligent Traffic Management System
IVD	Infraction Vehicle Data
IVR	Interactive voice response
IVRS	Interactive voice response system
JMS	Java Message Service
JPEG	Joint Photographic Experts Group
JPG	Joint Photographic Experts Group
JSON	JavaScript Object Notation

Acronym	Definition
JSR	Java Specification Requests
KMIP	Key Management Interoperability Protocol
KML	Keyhole Markup Language
KPI	Key Performance Indicator
KVA	Kilo Volt Ampere
KVM	Keyboard, Video and Mouse
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LBS	Location Based Services
LCD	Liquid Crystal Display
LDAP	Lightweight Directory Access Protocol
LDMP	Local Disaster Management Plan
LDR	Light-dependent resistor
LED	Light Emitting Diode
LHS	Left Hand Side
LIC	Life Insurance Corporation
LIFO	Last In First Out
LIG	Low Income Growth
LLDP	Link Layer Discovery Protocol
LPCB	Loss Prevention Certification Board
MAC	Media Access Control
MBPS	Megabytes per second
MCH	Maternal and Child Health
MDM	Mobile Device Management
METS	Metadata Encoding and Transmission Standard
MHZ	Megahertz
MIMO	Multiple Input Multiple Output
MIS	Management Information System
MJPEG	Motion Joint Photographic Experts Group
MMID	Mobile Money Identifier
MMS	Multimedia Messaging Service
MOM	Minutes of Meeting
MOP	Manual of Office Procedure
MPEG	Moving Picture Experts Group
MPLS	Multi-Protocol Label Switching
MRP	Material Requirements Planning
MSDG	Mobile Service Delivery Gateway
MSDP	Mobile e-governance Services Delivery Platform
MSI	Master System Integrator
MSSQL	Microsoft Structured Query Language
MSW	Municipal Solid Waste
MTA	Mail Transfer Agent
MTBF	Mean time between failures
MTTR	Mean Time to Repair
NABL	National Accreditation Board for Testing & Calibration Laboratories
NAC	Network Access Control
NAP	Network Access Point
NAS	Networked Attached Storage
NAT	Network Address Translation

Acronym	Definition
NCRB	National Crime Records Bureau
NDSAP	National Data Sharing and Accessibility Policy
NFC	Near Field Communication
NHAI	National Highway Authority of India
NIC	National Informatics Centre
NICT	New Information and Telecommunication technologies
NID	Network Identification
NIST	National Institute of Standards and Technology
NIT	Notice Inviting Tender
NMAM	National Municipal Accounting Manual
NMMP	National Mission Mode Project
NMS	Network Management System
NPCI	National Payments Corporation of India
NPL	National Physical Laboratory
NREGA	National Rural Employment Guarantee Act
NRW	Non Revenue Water
NTCIP	National Transportation Communications for Intelligent Transportation System Protocol
NVR	Network Video Recorder
OAIS	Open Archival Information Systems
OCR	Optical Character Recognition
OEM	Original Equipment manufacturers
OFC	Optical Fiber Cable
OGC	Open Geospatial Consortium
ONVIF	Open Network Video Interface Forum
OPC	Object Linking & Embedding for Process Control
OSD	On Screen Display
OSPF	Open Shortest Path First
OTA	Over the Air
OTP	One Time Password
PAR	Performance Appraisal Report
PAS	Public Address System
PAT	Prototype Acceptance Test
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation
PDF	Portable Document Format
PDFA	Portable Document Format for Archival
PDU	Power Distribution Unit
PEAP	Protected Extensible Authentication Protocol
PHEO	Public Health Engineer Organization
PIN	Personal Identification Number
PIO	Public Information Officer
PIT	Pre-Installation Testing
PLC	Programmable Logic Controller
PMC	Programme Management Consultant
PNG	Portable Network Graphics
POE	Power over Ethernet
POP	Point of Presence
POS	Point of Sale
PPB	Parts per Billion

Acronym	Definition
PPM	Parts per Million
PPR	Pre Project Report
PRI	Primary Rate Interface
PSIM	Physical Security Information Management
PTT	Push to Talk
PTZ	Pan,Tilt and zoom
PWC	Para wise comment
PWM	Pulse Width Modulation
QCIF	Quarter Common Intermediate Format
QSFP	Quad (4-channel) small form-factor pluggable
QVGA	Quarter Video Graphics Array
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RBI	Reserve Bank of India
RDA	Rourkela Development Authority
RDBMS	Relational Database Management System
REST	Representational State Transfer
RFID	Radio Frequency Identification
RFP	Request for Proposal
RFQ	Request For Quotation
RHEL	Red Hat Enterprise Linux
RHS	Right Hand Side
RIP	Routing Information Protocol
RLVD	Red Light Violation Detection
RMC	Rourkela Municipal Corporation
RMON	Remote Monitoring
ROM	Read Only Memory
RSCL	Rourkela Smart City Limited
RSPM	Respirable Suspended Particulate Matter
RTA	Regional Transport Authority
RTGS	Real Time Gross Settlement
RTI	Right to Information
SAIL	Steel Authority of India Limited
SAN	Storage area network
SAT	System Acceptance Test
SCIAA	State Environment Impact Assessment Authority
SIP	Session Initiation Protocol
SIT	System Integration Testing
SLA	Service Level Agreement
SMPS	Switched Mode Power Supply
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedure
SPCB	State Pollution Control Board
SPV	Special Purpose Vehicle
SQL	Structured Query Language

Acronym	Definition
SRS	Software Requirement Specifications
SSD	Solid-State Drive
SRTP	Secure Real Time Protocol
SSO	Single Sign-On
STI	Speech Transmission Index
STP	Spanning Tree Protocol
STQC	Standardisation Testing Quality Certification
TACACS	Terminal Access Controller Access-Control System Plus
TAT	Turn Around Time
TCC	Traffic Command Centre
TCP	Transmission Control Protocol
TCPS	Technical Control and Processing Section
TCS	Tata Consultancy Services
TDE	Transparent Data Encryption
TDR	Transferrable Development Rights
TDS	Tax Deducted at Source
TFA	Treated Fresh Air
TFT	Thin Film Transistor
TGT	Trained Graduate Teacher
THD	Harmonic Distortion
TIA	Telecommunications Industry Association
TIFF	Tagged Image File Format
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOR	Terms of reference
TRAI	Telecom Regulatory Authority of India
TRD	Test Results Documentation
TSN	Time Since New
TSO	Time Since Overhaul
TSP	Telecom Service Provider
TSV	Tab Separated Values
TTF	True Type Fonts
TTS	Text to Speech
TVD	Traffic Violation Detection
TVDS	Traffic Violation Detection System
UAN	Unique-Account-Number
UCS	Unified Communication System
UDL	Uniformly Distributed Load
UHF	Ultra-High Frequency
UID	Unique Identification Number
UIDAI	Unique Identification Authority of India
ULB	Urban Local Bodies
ULC	Underwriters Laboratories Canada
UMTS	Universal Mobile Telecommunications System
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
USSN	Unstructured Supplementary Service Notify

Acronym	Definition
USSR	Unstructured Supplementary Service Request
VaMS	Variable Message Signboard
VAS	Value Added Services
VAT	Value Added Tax
VBR	Variable Bit-Rate
VCR	Video Cassette Recorder
VGA	Video Graphics Array
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VMS	Video Management System
VOIP	Voice over Internet Protocol
VPLS	Virtual private LAN service
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VRLA	Valve Regulated Lead Acid
VRRP	Virtual Router Redundancy Protocol
VSC	Voice Security Card
VTG	Virtual Talk Group
VTP	VLAN Trunking Protocol
WAF	Web Application Firewall
WAN	Wireless Access Network
WAV	Waveform Audio File Format
WBS	Work Breakdown Structure
WDR	Wide Dynamic Range
WEEE	The Waste Electrical and Electronic Equipment (Directive)
WESCO	Western Electricity Supply Company of Odisha
WIG	Wireless Internet Gateway
WIP	Work in Progress
WIPS	Wireless Intrusion Protection System
WLAN	Wireless Local Area Network
WLC	Wireless LAN Controller
WML	Wireless Markup Language
WMS	Wireless Management System
WSDL	Web Services Description Language
WSRP	Web Services for Remote Portals
XLS	Excel Spreadsheet (Microsoft file Extension)
XML	Extensible Markup Language

Background and Scope of Work

Background

Rourkela is the 3rd largest city of Odisha after Bhubaneswar and Cuttack, located in Sundargarh district with a population of around 4.83 lakh as per the Census of India, 2011. Rourkela is primarily an industrial town lying in the midst of an important mineral belt in the country. In terms of connectivity, Rourkela is well connected through rail network with other parts of the country. Also, the city is likely to have air connectivity with select cities, including Bhubaneswar and Kolkata shortly.

Rourkela is one of the 99 smart cities selected under the Smart City Challenge in September, 2016 by Ministry of Housing and Urban Affairs. As mentioned in the SCP, the city has set its vision as follows:

*"Building on its **steel foundation, natural setting** and **cosmopolitan character**, Rourkela - a prominent eastern Indian city located **in the heart of tribal belt** renowned for producing ace **sporting talent**; will be a **liveable, inclusive, sustainable** and **self-reliant** city, propelling the **regional economic development** with best in class **future proof infrastructure**".*

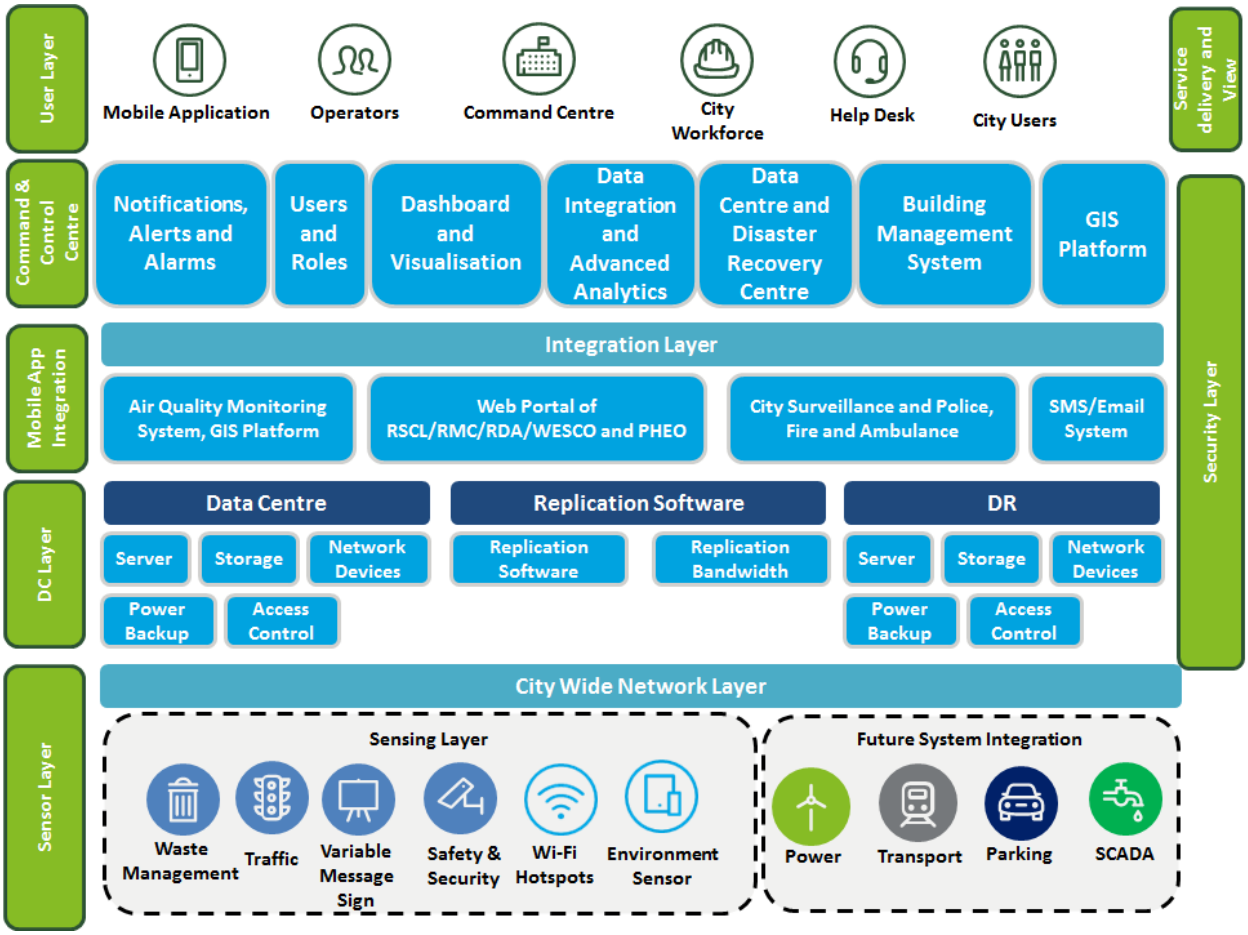
No.	Project Module	Name of Project
1	Swachh Rourkela/ Waste Management	Waste Management system comprising RFID / sensors tagged waste bins, GPS based waste collection/cesspool vehicles with RFID readers and vehicle tracking & monitoring system
2	Paribahan/ Traffic Management	Adaptive Traffic Signal Control System
		Traffic Violation Detection System
3	City Governance	e-Governance (Urban services for Citizens)
		Smart City App
		City Surveillance System
		Citizen Facilitation Centre's/ e-Kiosks
4	Other Smart Elements	Variable Message Signboards (VaMS) and Public Address System (PAS)
		Smart Wi-Fi
		Environment Monitoring System
		Smart Classroom

In addition to the smart components highlighted above, an Integrated Command and Control Centre (ICCC) is proposed for integration of various services for purpose of monitoring and analysis.

This document highlights the key projects / solutions proposed as highlighted above and provides all requisite details required for the MSI to understand and accordingly prepare and submit the proposal.

Scope of Work

The MSI shall be responsible for implementing an end to end solution for city of Rourkela which comprises the following:



Sensor and Actuator layer

The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like emergency call boxes, cameras, RFID tags installed on the bins, etc. Rourkela city is expected to have multiple environmental sensors across the city, to measure ambient conditions such as light intensity, temperature, air pollution, noise pollution and humidity.

Network Layer

The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. It will support the Wi-Fi services and other smart elements (sensors and displays) at given locations. The network layer will be scalable such that additional sensors, actuators, display devices, etc. can be seamlessly added in future. The MSI will enter into a suitable arrangement with a telecom service provider to provide required network connectivity for implementing the solutions.

Data Center Layer

The data center layer will house centralized computing power required to store, process and analyse the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. Similar to the network layer, it will be scalable to cater to the increasing computing and storage needs in future.

Smart Application and Integration Layer

The smart applications layer will contain data aggregation and management systems (rules engines, alerting systems, diagnostics systems, control systems, messaging system, events handling system), and reporting /

dashboard system to provide actionable information to city administrators and citizens. It will be an evolving layer with applications added and integrated as and when new applications are developed. While aspects of ambient conditions within the city will be gathered through various sensors deployed, some city specific data will come from other government and non-government agencies. It is through the integration layer that data will be exchanged to and from the underlying architecture components and other data from systems developed by government (such as Municipal Corporation of Rourkela, police department, state pollution control board, street lights department, water department, irrigation department within Rourkela, etc.) and quasi/ non-government agencies.

Service delivery and consumption Layer

This layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume and for administrators to provide actionable information. Such field devices include CCTV cameras, adaptive traffic signals, digital messaging boards, environmental data displays, e-Kiosks etc.

Control Units & Command Center Layer

The command center and control units will enable citizens and administrators to get a holistic view of city conditions. Such control units will take shape of either an exhaustive command center or control applications which can be viewed over a web browser or available in form of a mobile application. The implementation vendor will have to develop a command center at a site location determined by RSCL and web/ mobile based viewing tools for securing a holistic view of city conditions.

Security Layer

As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance and the system integrator will have to provide:

- Infrastructure security - including policies for identity and information security policies
- Network security - including policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources, etc.
- Identity and Access Management – including user authentication, authorisation, SSL & Digital Signatures
- Application security - including Hosting of Government Websites and other Cloud based services, Adoption of Technical Standards for Interoperability Framework and other standards published by Government of India (GOI) for various e-Governance applications
- End device security, including physical security of all end devices such as CCTV cameras, adaptive traffic signals, digital messaging boards, environmental data displays, e-Kiosks etc.
- Following security parameters should be included for all smart elements, but not limited to:
  - Identity and access management
  - User/administrator audit log activity (logon, user creation, date-time of PA announcements, voice recording etc.)
  - Secured data storage (storage of video/image/voice/location/data captured by various smart elements)
  - SSL/TLS encryption for web and mobile application based interfaces for sensitive data transfer
  - Protection against Denial of Service (DoS) and Interference attacks to public Wi-Fi Devices

Survey and Detailed Design of all Smart Solutions

MSI shall conduct end-to-end survey of the site area, additional requirement gathering and based on the observations, asses and validate the present conditions, project challenges and mitigations and other project critical information. During the survey stage itself, MSI shall mobilize its entire staff and fully acquaint them with the site conditions. The MSI will survey the sites and assess conditions for planning and designing the implementation. During the design validation stage, MSI is also expected to:

- Conduct workshops with different stakeholders for capturing business requirements, creating awareness of best practices, communicating the changes, building consensus on process design etc. These needs to be organized at different intervals and in different places throughout the duration of the projects as needed.
- Hold stakeholder consultations other than workshops, with those stakeholders who will be identified by RSCL, for critical inputs, review, suggestions, process description etc.

- Conduct review sessions with different stakeholders for signing off the deliverables, walking through the deliverables for facilitating quick understanding.
- For network connectivity, the MSI shall carry out a gap analysis in order to capture the WAN and Local connectivity requirements. The analysis should also cover the detailed network related requirements of IT and Non IT infrastructure at each location.

The MSI shall also be responsible for obtaining necessary concurrence on the detailed project design. MSI shall discuss in detail and validate with the Client or its representatives the detailed design of the smart city ICT components and fine tune any requirements. It is the MSI's responsibility to satisfy the operational requirements of the Client and adopt industry best practices for implementation during the design stage itself. Based on the survey observation, analysis and discussion with the Client, the MSI shall submit a Detailed Design Report. The detailed design report shall include end-to-end design validation for the project including any project understanding, analysis, detailed design, integration plan, and for-construction drawings. Complete set of design and construction drawing including method of installation as applicable shall also be included in the Detailed Design Report. Construction details shall accurately reflect actual job conditions.

All technical data sheets of the products may be submitted ahead of time by the MSI. It is MSI's responsibility to get all technical data sheets approved by the Client or its representative to meet the overall project schedule.

While designing the solution, MSI is expected to consider the aspect of scalability without any additional cost in terms of hardware, software (Licenses) and services to add additional smart elements like

- Additional sensors/IoT devices for future/new requirements (Approximately 20% increase in the total devices connected) [Example SCADA integration with Downstream applications related to Water management, Electricity, Monitoring of Public Transport, Parking, Sewage, etc.]
- Standards based integration for future/new requirements with applications like eGov applications and related apps, third party systems (Through Open API's for additional Applications)
- Helping RSCL in finding solution for new challenges faced in day to day scenario by customizing the existing smart solutions.

The design of the entire Smart City Solutions (which would serve as a basis for implementation subsequently) should comply with Good Industry Practices and at a minimum follow the design principles and standards highlighted in Annexure-A

Design and construction drawings shall include the following at a minimum:

- All system device locations as required for installation, operation and maintenance
- Cable requirements, routing and location (as applicable)
- Typical mounting details
- Single Line Diagrams (SLDs)
- Splicing diagrams
- Wiring diagrams
- 3D layouts and renderings for POP and ICCC Hall
- Any other layouts including legacy equipment details ,if any
- Any other requirement to meet the requirements of the RFP

All drawings shall be updated/revised to "as-built" conditions when installation is complete.
Design submissions shall be based on project requirements and shall include as applicable, but not limited to, the following:

- Complete listing of specifications to be used along with detailed technical data sheet
- Detailed engineering drawings
- Shop drawings including product data sheets
- Revisions to original design submissions

No work requiring shop drawing submission shall commence until final review has been obtained by Client. However, review of the shop drawings by the Client shall not relieve the MSI of its responsibility for detailed design validation inherent to shop drawings.

For the software components, MSI will create requirement analysis documents for various components of the solution. This includes System Requirements Specification (SRS) and Functional Requirements Specification

(FRS) documentation. The MSI shall be responsible for documenting any existing/planned 'processes' of the Client as part of these deliverables.

This detailed design report shall be submitted to RSCL for all the phases of the project.

Prototype acceptance and factory testing

Post approval of the detailed design, MSI shall develop the prototype of all the components/solutions and obtain the Client's approval. It shall be MSI's responsibility to get the prototypes approved in due course of time without affecting the overall schedule of completion.

Components/solutions provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT) as per Project Plan. Details regarding the PAT and FAT are presented in Testing Section of the Scope of Work. MSI shall also present to the Client and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The client at its own discretion shall visit any FAT site. MSI shall be responsible for organizing all logistics required for this site visit. For all the software components, MSI shall also propose prototype of solution components in this phase and get the required approvals.

Hardware Supply and Installation

MSI shall be responsible for the supply and installation of all components as part of the smart city ICT components to meet the technical, functional, business and performance requirements of the RFP. No deviations from these requirements shall be acceptable by the Client. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and provided by the MSI. MSI shall deliver the project and install and handle the equipment in accordance with manufacturer's requirements. Installation process of the MSI shall be flexible and shall accommodate Client's requirements without affecting the schedule as specified in the RFP.

MSI shall be responsible for all supply, storage and handling of the material provided as part of the project. The OEM proposed for the IT infrastructure shall adhere to applicable national/ state security policies.

If there is removal/change of any existing material during installation process, the material shall be handed-over to the Client. It shall be the MSI's responsibility to supply and install all hardware in compliance with the requirements of the RFP. MSI shall be responsible for all implementation works on the project including any civil, structural, electrical, etc. works required to meet the requirements of the project. All power conversions necessary to operate the equipment shall be under the scope of MSI.

Software Development

MSI shall be responsible for development and deployment of all software required to meet the requirements of the project. Some of the software may be "Commercial Off-The-Shelf (COTS)" or may require bespoke development as outlined in the subsequent sections of this document. MSI shall be fully responsible for developing, implementing, integrating and maintaining all the software required for the project. All software development/implementation should be developed using standard Software Development Life Cycle (SDLC) with suitable checkpoints at the end of each activity and may be demonstrated to the client periodically as per the project requirements. All software shall be developed based on the approved software and functional requirements specifications. The technology platform chosen for all software shall be based on open standards and shall be secure. Migration of data shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration.

The MSI shall ensure that full support from the OEMs' are provided during the course of the contract. MSI shall be responsible to provide any upgrades, patches, fixes to the software during the course of the contract at no additional cost to the client.

Pilot Deployment

The MSI shall conduct Pilot deployment and testing for meeting Client's business requirements before rolling out the complete system. The pilot will be operated for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the pilot implementation until it has stabilized. Based on Client's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.

The Pilot shall be demonstrated to the Client's representatives. If for any reason during the pilot implementation, the solution or components thereof does not meet the client requirements, these will be communicated to the MSI in writing. A one-time extension will be provided to the MSI to correct the lapses pointed out before offering the upgraded pilot to Client for review. Failure to successfully demonstrate all required functionalities during pilot implementation shall lead to termination of the contract with no liability to Client.

Testing

All materials, equipment, systems, manufacturing or configuration processes, or other items to be provided under the Contract shall be inspected and tested in accordance with the requirements specified in this document and will be subject to Client or its representative's approval. The testing shall include any existing civil infrastructure equipment or materials to be taken over by the MSI. Approvals or passing of any inspection by the Client shall not, however, prejudice the right of the Client or its representative to reject the material if it does not comply with the specification or requirements of the RFP when erected or give complete satisfaction in service.

The MSI shall design and successfully complete tests to demonstrate that all equipment, materials and systems furnished and installed function in the manner intended and in full compliance with the requirements outlined in the RFP and the approved detailed design of the MSI.

All tests shall be subject to inspection or witnessing of tests by the Client or its representative. Inspection or witnessing of tests may be waived at the sole discretion of the Client or their representative, subject to the MSI furnishing the Client or their representative with properly completed test certificates in accordance with the requirements of the RFP. Failure of the Client or their representative to witness any test shall not relieve the MSI of the obligation to meet the requirements of the Contract.

MSI shall submit an Acceptance Test Procedures document (ATP), for Client's approval prior to undertaking any testing. The ATP shall clearly address:

- Type of testing and device to be tested;
- How each testable specification requirement will be demonstrated, including the test environment and set-up, specific functionality to be tested, method for performing the test and quality assurance procedures;
- The results that will constitute success for each test;
- Timing of test within the overall Contract schedule;
- The location for testing;
- Personnel required to conduct the test;
- Approximate time required to execute the test or set of tests;
- Responsibilities of both the MSI and Client's representatives during each test; and
- A cross-reference to which Contract requirements from the Compliance Matrix (to be developed by the MSI) are being addressed by each test procedure.

The ATP shall include an updated Compliance Matrix to include the test relevant stage at which each contract requirement will be demonstrated; and a cross-reference to the test procedure(s) that serve to address each contract requirement. The Compliance Matrix shall be used as a "punch list" to track which requirements have not yet been demonstrated at each stage of testing. A requirement classified as having been "demonstrated" during a certain ATP stage can be subsequently redefined as having been "not demonstrated" if compliance issues emerge prior to System Acceptance. ATP shall be submitted to Client at least three (3) weeks in advance of any intended testing.

All measuring instruments required to measure test parameters shall be calibrated by an approved testing

authority. The equipment shall be inspected for standards of construction and electrical and mechanical safety.

Test results shall be recorded for all tests conducted under this Contract. The MSI shall make test results available to Client or their designate for review immediately after completion of the tests.

ATP for each test shall be collated, bound and delivered as part of the close-out documentation requirements specified herein.

ATP submission shall include a hard copy of the originally marked test results and a neatly typed summary. Two (2) hard copies and one (1) electronic copy shall be provided.

ATP shall incorporate the following distinct stages for each deployed component/solution:

- **Prototype Acceptance Tests (PAT)**: Prototype Approval Test shall be conducted only on the customized component/solution for their design and compliance to functional specifications. PAT shall be completed before conducting FAT and only after approval of PAT by Client's representative, the solution shall go in production. PAT shall be witnessed by Client's representatives;
- **Factory Acceptance Tests (FAT)**: FAT shall be conducted before the component/ solution is shipped to Client for installation, and deficiencies shall be rectified before shipping to Client for installation. All solutions furnished by the MSI shall be tested and subjected to a nominal 72-hours burn-in period at the factory. FAT shall be witnessed by Client's representatives at their discretion. Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected;
- **Pre-Installation Testing (PIT):** All component/solution supplied under this Contract shall undergo pre-installation testing in accordance with the ATP. This shall include existing component/solution, any spare parts, any new component/solution provided by Client or their designate and new component/solution provided by the MSI.

  All PIT testing shall be carried out prior to installation of the component/solution. After satisfactory completion of the MSI's PIT tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.

  If the component/solution is considered a standard production item, the MSI may, with the prior consent of the Client or their designate, supply a copy of the component/solution manufacturer's quality control test results in place of a MSI performed test.
- **Installation Acceptance Tests (IAT)**: IAT shall be conducted after each installation of each component/solution type, and deficiencies shall be rectified before the initiation of SAT. IAT may be witnessed by Client's representatives;
- **Proof of Performance Testing (POP):** The MSI shall implement a structured proof of performance testing, which will progressively place all components in service. Site tests shall be performed on individual components, subsystem sites, and the complete subsystems, as necessary to confirm that each element of the system functions satisfactorily and fulfils the requirements of this specification.

  Completion, submission, and approval of all relevant PIT and IAT tests and results must be completed prior to carrying out any POP tests.

  All subsystems and components shall be tested by the MSI regardless of whether or not it is a standard item.

  After satisfactory completion of the MSI's POP tests, the MSI shall supply all test measurements and results to the Client or their designate, together with a Test Certificate.
- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to

existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the Client or their designate. This work will be carried out under the direction of the Client or their designate.

Completion, submission and approval of all relevant PAT, FAT, PIT, IAT and POP tests and results must be complete prior to carrying out any SIT tests. The MSI shall:

- Complete all equipment and subsystem tests required in the Contract;
- Test each subsystem independently on the communications subsystem;
- Add subsystems one at a time and monitor the overall performance;
- Fail safe testing of all subsystems one at the time while monitoring overall systems performance.

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system, together with final copies of all Operating and Maintenance Documentation for the System.

- **Stress and Load Testing:** Comprehensive stress and load testing of all component/solution shall be conducted to demonstrate robustness and reliability of the system.
- **Security Testing (including penetration and vulnerability test):** Security test shall be conducted to demonstrate security requirements at network layer and software applications. Components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for portal, mobile app, and other systems. Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.
- **Pilot Test:** Requirements for Pilot Test is explained in the Pilot Deployment Section of the Scope of Work.
- **System Acceptance Tests (SAT):** SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of Burn-in Test. SAT shall be conducted on full system completion only to determine if the system functional and technical requirements as specified in the bidding documents are met. SAT shall be witnessed by Client's representatives. Data migration, if any will be carried out by MSI prior to commencement of this stage. SAT shall also include any performance and load testing for the software applications.

  SAT should include End to End (E2E) Testing which shall be conducted to certify the implementation of business processes in its entirety. E2E testing will cover all business flows and connectivity with all the interfacing systems. No mock setup will be used for integrations during the testing phase, since all the interfaces are expected to be available for validations. The test scenario matrix will need to be prepared that provide details of the following:
  - Detailed description of the scenario with the associated business process across Upstream Applications & Downstream Applications
  - All Applications, interfaces listed in scope of the program – a checklist to indicate whether the scenario will traverse through the identified system(s)

The entry/exit criteria for the SIT and E2E testing and its deliverables are provided in the table below:

Entry Criteria	Exit Criteria	Deliverables
• System Integration Testing complete for all interfacing applications • E2E Test scenarios / cases are reviewed and signed off by SMEs (Subject Matter	• 100% of planned test cases are executed and test results are documented • 100% pass rate on executed test cases	• End to end test scenarios and test cases • End to end defects report • End to end test execution evidence

Entry Criteria	Exit Criteria	Deliverables
Expert)/ SPV • No blocker / critical defects in open status from ST/SIT phases • Known defects (open status) are documented clearly from ST/SIT phases	• No blocker / critical defects in open status • Known defects (open status) are documented clearly • Sign off on the test results	• End to end test summary report

- **Burn-in Tests (BT)**: Following successful completion of the SIT and SAT, the approved System will be put into service and its performance monitored for a period of thirty (30) consecutive calendar days for the purpose of verifying system reliability in an operating environment. Any failures and defects occurring in this time will be documented. Any serious defects which affect the availability of the system will be a basis for restarting the test. Upon the satisfactory completion of this performance testing, a Completion Certificate will be issued.

The MSI shall not commence BT until SIT and SAT have been performed and successfully completed and all documentation of the successful completion of PAT, FAT, PIT, IAT, POP, SIT and SIT, along with notification of the schedule date of the BT is provided to the Client or their designate in accordance with the requirements. Commencement of BT will be conditional on the Client or their designate providing written notification of Client's readiness to proceed to BT.

The MSI shall be suitably prepared for the BT prior to the start date. Repeated failure of the BT may result in the MSI having to reimburse the Client or their designate for costs incurred. No compensation to the MSI will be made for repeat testing.

Where equipment supplied by the MSI fails during the burn-in period, the MSI shall restart the test at day zero (0) following appropriate corrective measures.

If a utility failure is proved to be the cause of testing failure, then the MSI shall restart the fourteen (14) day burn-in test at the day the failure occurred. If a subsystem failure is proved to be the cause of testing failure, then the MSI shall start the test over at day 0 (zero).

Where tests or burn-in indicate that an existing subsystem or component, not provided by the MSI, is defective, the MSI shall immediately report the deficiency to the Client or their designate. The Client or their designate may assign corrective repairs, retesting and repeat of BT to the MSI, in accordance with the changed provisions of the Agreement.

The MSI shall provide the Client or their designate with a contact name and phone number(s) for a designated emergency contact person during BT. The emergency contact person shall be accessible twenty-four (24) hour a day, for each day of testing.

- **Operational Acceptance Test:** Shall be conducted after successful SAT and Burn-in tests. Continuous fault free running of the System shall be tested. Post the completion of Operational Acceptance Test, System shall be considered for Operational System Acceptance and Defect Liability Period (DLP) shall commence. Operational Acceptance Test shall include the following as a minimum:
  - Completion of all activities and fulfilment of all business, functional and technical requirements listed in RFP;
  - Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc.;

Client may authorize the MSI to proceed to the next testing stage with certain deficiencies not yet resolved.

In case of failure of any component, the component in question shall be repaired and the test shall be reconducted. If a component has been modified as a result of failure, that component shall be replaced in all like units and the test shall be reconducted for each unit.

MSI shall provide the Client with a copy of the manufacturer's quality assurance procedures for information. Documentation certifying the showing that each item supplied has passed factory inspection shall also be submitted by the MSI.

The MSI shall provide written notice to Client at least five days in advance of any testing, indicating the specific tests to be completed as well as the date, time and location. The MSI shall be required to reschedule testing if Client witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

MSI shall provide written Test Results Documentation (TRD) within one week of completing each stage of testing. The TRD shall document the results of each ATP procedure and provide an updated Compliance Matrix that indicates which contract requirements have been demonstrated. The TRD must be approved before Client will grant System Acceptance. A sample format for the TRD is provided below:

Item #		**Test:**	
Item Description		**Date:**	
Test Set-up:			
Clause	**Test Procedure**	**Expected**	**Actual Results**
Witnessed (This Does Not Constitute Approval): **Reviewed and Approved:**			

MSI shall be responsible to carry out all the testing as per the satisfaction of the Client and its representatives. All costs associated with any testing are to be borne by the MSI including the costs of travel and accommodation of the Client or its representatives from their home locations in their cost bid. A maximum of three (3) people shall be nominated by the Client to attend any such testing wherever it is carried out.

STQC Certification and Audit

Each of the Functional Requirement and the Technical Requirement shall be assessed and audited by the STQC, Government of India as per existing scope of the MSI with the MSI engaging the STQC at various stages along the implementation and satisfactory clearance of the system(s) by the STQC in terms of the Physical, Performance and statutory compliances as per scope.

MSI is responsible for getting the STQC certification for the solutions that are part of this RFP.

All the software systems/solutions that are in scope of MSI shall go through STQC Audit, security vulnerabilities detected by the STQC shall be fixed by the MSI and further should be submitted for STQC and receive the clearance.

Further software systems/solutions that are in scope of MSI shall be performance audited by the STQC for standard or best practices performance of application flow and processing.

Software systems/solutions that are in scope of MSI shall comply with the Government of India guidelines as per the details in STQC site (http://www.stqc.gov.in/content/information-security-testing-and-assessment)

No product or service shall be hosted in the ICCC / or other APP stores or paid for unless these are certified cleared by STQC India as per their standard tests.

System Integration

MSI shall be responsible for the integration of all hardware and software supplied as part of this Project as per the technical and performance requirements of the project. The system integration scope also includes integration of the Project components with the components provided by others as per the details of the RFP. It shall be the responsibility of MSI to take approval of the Client for the Integration of the overall system as per the RFP. Post systems integration, the Client shall review and approve the overall performance of the integrated system as per the requirements of the RFP. MSI shall be responsible for fixing any requirements that are not found in compliance with the original RFP and approved detailed design at no additional cost to the client within the agreed SLA.

Project Management

MSI shall be responsible for providing end to end project management for implementation and maintenance of the smart city ICT components. MSI shall deploy team of experts for project management.

The Project Manager shall be the single point of contact and shall assume overall responsibility of the Project to ensure end to end working of the Project. The Project manager shall function as the primary channel of communication for all Client requirements to the implementation team. In case of any absence of the project manager (vacation or sickness), the MSI shall ensure that an alternate project manager (of similar or better qualification) is present on site during the absence period of the proposed Project Manager.

MSI shall be responsible for preparing a master schedule of work which shall highlight implementation plan for all the Project milestones. The schedule shall identify manufacture, delivery, installation, integration of equipment (Software and Hardware), training programs, test procedures, delivery of documentation for respective solutions and final handover. The schedule shall also show Client and any third party responsibilities along with the activities in the timeline. MSI shall conduct bi-weekly meetings between the Client (and / or its representative) and the 'key personnel' to discuss project progress and implementation at desired location. All key personnel associated with the project shall also be available for meetings whenever asked by the Client or its representative.

MSI shall also be responsible for effective risk and issue management and escalation procedures along with matrix as part of project management. MSI shall identify, analyses, and evaluate the project risks and shall develop cost effective strategies and action plan for mitigation of risks. As part of the Project, MSI shall monitor, report and update risk management plans which shall be discussed during project meetings.

MSI shall prepare minutes of every meeting which takes place and submit to Client or its representative for tracking of the Project. MSI shall propose a suitable progress reporting mechanism for the project duration.

All the tools required by MSI for project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI.

Based on progress reports, MSI shall also accordingly update the master schedule of work on a continuous basis during the period of the contract.

All deliverables shall be submitted in at least two (2) formats i.e. draft and final. The Client's representative will have maximum 15 days to review and comment on every deliverable. The practice of submissions for all deliverables will be that three (3) hard copies and CDs of every deliverable shall be submitted. Two of these copies will be submitted to the Smart City PMC and one will be submitted to the client. The submissions will include both hard and soft copies.

Change Management and Training

In order to strengthen the staff, structured capacity building programmes shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for Command Control Centre, City Operation Staff and designated Rourkela Municipal Corporation (RMC) & Police staff shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of ICCC. These officers shall be handling emergency situations with very minimal turnaround time.

- MSI shall prepare and submit detailed Training Plan and Training Manuals to purchaser/authorized entity for review and approval.
- Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
- MSI shall be responsible for necessary demonstration environment setup including setup of cameras, Wi-Fi, kiosk and other required solutions to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at ICCC, ITMS, Safety and Surveillance, City Governance, DC and other smart solutions. End user training shall be conducted at a centralized location or any other location as identified by purchaser with inputs from the MSI.
- MSI shall conduct end user training and ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system.
- MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.

- MSI shall prepare the solution specific training manuals and submit the same to purchaser for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
- MSI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.
- MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
- An annual training calendar shall be prepared and shared with the Client along with complete details of content of training, target audience for each year etc.
- MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
- The MSI shall ensure that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by the MSI.
- Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the MSI.
- Time Schedule and detailed program shall be prepared in consultation with RMC and respective authorized entities (like Police Department, OPCB among others). In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
- MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- Client shall be responsible for identifying and nominating users for the training. However, MSI shall be responsible for facilitating and coordinating this entire process.
- MSI shall be responsible for making the feedback available for the Client/authorized entity to review and track the progress, In case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the MSI shall re-conduct the same training at no extra cost.

Types of Trainings

Following training needs are identified for all the project stakeholders:

Basic IT training:

This module shall include components on fundamentals of train the trainer basis:

- Computer usage
- Network connection troubleshooting
- Smart phone/ Tab usage with respect to smart city solutions
- Application user administration
- Application installation & troubleshooting
- Basic computer troubleshooting etc.

Initial Training as part of Project Implementation:

- Functional Training
  - Basic IT skills
  - Video Management Software, Video Analytics, etc.
  - Software Applications (City Operation Center and Command & Control Center)
  - Mobile Surveillance Vehicle
  - Mobile Command and Control Center (Integrated Command Center over field devices)
  - Networking, Hardware Installation
  - Centralized Helpdesk
  - Feed monitoring

  - Any other relevant training
- Administrative Training
  - System Administration Helpdesk, Facility Management System (FMS), Building Management System (BMS) Administration etc.
  - Master trainer assistance and handling helpdesk requests etc.
- Senior Management Training
  - Usage of all the proposed systems for monitoring, tracking and reporting,
  - MIS reports, accessing various exception reports

Post-Implementation Training

- Refresher Trainings for the Senior Management
- Functional/Operational training and IT basics for new operators
- Refresher courses on System Administration
- Change Management programs
- Training to the employees of Rourkela Smart City Limited and it's appointed agencies on application related operations and basic troubleshooting & reports generation etc.

MSI will have to bear all the cost associated with the conducting such training programs. However, the space for such trainings shall be provided by the Client

Training sessions should be conducted on a requisite mix of theory & practical operations. The trainings should be conducted in English, Hindi and Odiya languages as applicable.

Initially the bidder will be required to impart training to the personnel designated (approx. 20 nos.) by Rourkela Smart City Ltd. for one month, thereafter a similar training will be repeated once every quarter for the contract duration.

MSI has to provide application and role based training to the ICCC operators and supervisors of different applications like VMS, ICCC, Video Analytics and forensic Software

Full Deployment, Documentation and Handover

Post the final deployment, MSI shall handover detailed documentation that describes the site conditions, system design, configuration, training, as-built conditions, operation and maintenance. All documentation shall be in English, shall utilize metric measurements, and shall be submitted directly to Client in paper hardcopy and electronically in Word/ AutoCAD/ Excel/ Project and Adobe Acrobat.

All installation drawings shall be prepared in AutoCAD, GIS and Adobe Acrobat and provided on CD-ROM as well as hard copies. The drawings shall contain sufficient detail including but not limited to equipment dimensions, interfaces, cable details, equipment mounting and fire protection.

Electrical and electronic drawings shall be supplied to show engineering changes made to any component or module any time during the contract period.

The MSI will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. The indicative documentation to be submitted across various stages of implementation are as follows:

- **Project Commencement Documentation:** Project Plan in giving out micro level activities with milestones & deadlines.
- **Cabling Layout:** Systems Integrator shall submit the detailed cabling layout including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways.
- **Equipment Manuals:** Original Manuals from OEMs.
- **Installation Manual:** For all the application systems
- **Training Material:** Training Material will include the presentations used for trainings and also the required relevant documents for the topics being covered. Training registers should be submitted for same.
- **User Manuals:** For all the application software modules, required for operationalization of the system.
- **System Manual:** For all the application software modules, covering detail information required for its administration.

- **Standard Operational Procedure (SOP) Manual:** The Bidder shall be responsible for preparing SOP Manual relating to operation and maintenance of each and every service as mentioned in this Tender. The draft process (SOP) document shall be formally signed off by Authority before completion of Final Acceptance Test. This SOP manual will be finalised by the Bidder within 2 months of operationalisation of each phase, in consultation with the Authority and formally signed off by the Authority.
- An inventory of all components supplied (Hardware, Software, Other equipment's including physical fitments) including model name, model number, serial number and installation location
- All reference and user manuals for system components, including those components supplied by third parties
- All warranties documentation, including that for components supplied by third parties
- As-built in CAD and GIS
- A diagram indicating the as-built inter-connections between components
- Software documentation which also includes the version number of all software, including that supplied by third parties
- Cable run lists and schedules
- All network and equipment details such as IP addresses, user names, and passwords
- Manufacturer's test procedures and quality assurance procedures for information
- Data communication protocols
- As-Built' drawings for all components installed.

MSI shall submit to the Client copies of comprehensive operating and maintenance manuals for all systems and hardware supplied as part of this bid document. The manuals shall be complete, accurate, up-to-date, and shall contain only that information that pertains to the system installed. Maintenance documents shall include:

- Equipment installation and operating documentation, manuals, and software for all installed equipment
- System Installation and setup guides, with data forms to plan and record options and configuration information
- The schedule/procedures for preventative maintenance, inspection, fault diagnosis, component replacement and on-site warranty support administration on each system component
- Hard copies of manufacturer's product specification sheets, operating specifications, design guides, user's guides for software and hardware, and PDF files on CD-ROM or non-volatile memory stick of the hard-copy submittal
- Complete list of replaceable parts including names of vendors for parts not identified by universal part numbers
- Manufacturer's product specification sheets, operating specifications, design guides, user's guides
- Permits
- Contractor names and telephone number, email address, escalation matrix with contact lists for all project trades.

MSI shall provide Systems Manuals (SM), documentation including:

- The configuration and topology of central systems hardware and software
- Central systems software functions and operations
- Scheduled maintenance required for the central systems
- Database structure and data dictionary

MSI shall also provide following documents for any be-spoke software development, if any:

- Business process guides
- Program flow descriptions
- Architecture details
  - System Architecture
  - Technology Architecture
  - Deployment Architecture
  - Data Architecture
- Data model descriptions
- Sample reports

- Screen formats
- Frequently Asked Questions (FAQ) guides
- User Manuals and technical manuals
- Any other documentation required for usage of implemented solution

Documentation of processes shall be done using standard flow-charting software.

All pages of the documentation shall carry a title, version number, page number and issue date, and shall contain a complete subject index. MSI shall be responsible for fully coordinating and cross referencing all interfaces and areas associated with interconnecting equipment and systems.

Documentation shall require re-issues if any change or modification is made to the equipment proposed to be supplied. MSI may re-issue individual sheets or portions of the documentation that are affected by the change or modification. Each re-issue or revision shall carry the same title as the original, with a change in version number and issue date.

Each volume shall have a binder (stiff cover and spine), and drawings shall be protected by clear plastic to withstand frequent handling. The binding arrangement shall permit the manual to be laid flat when opened.

Soft copies of the above documents (Word, pdf, Visio etc..,) has to be provided by MSI.

The paper used shall be of good quality and adequate thickness for frequent handling.

Operations Related Documentation

The MSI shall support RSCL in (not limited to)

- Preparing the reports/documents generated as per the end user requirement
- Exporting the same in standard format (pdf, csv, xlsx, doc, JSON objects etc.,)
- Printing the required reports

Note: MSI will ensure upkeep & updation of all documentation and manuals during the contractual period. The ownership of all documents, supplied by the MSI, will be with the Client. Documents shall be submitted in two copies each in printed (duly hard bound) & in softcopy formats.

Operational System Acceptance

Post go live, the system shall be considered for operational system acceptance. At the close of the work and before issue of final certificate of completion by the Client, the MSI shall furnish a written guarantee indemnifying Client against defective materials and workmanship for a period of one (1) year after completion which is referred to as Defect Liability Period. The MSI shall hold himself fully responsible for reinstallation or replace free of cost to Client during the Defect Liability period. MSI should also perform the operational aspects as mentioned in earlier section of this document. MSI shall provide approved temporary replacement equipment and material such that the system remains fully functional as designed and commissioned during repair or replacement activities at no cost to the Client.

The MSI shall support RSCL in day to day operations related to smart city (Software Configuration, Customization, Infra etc.) the scope of the same is briefly described below but not limited to

- Ensuring that all the Smart elements are up and running
- Ensuring that all the Smart solutions are properly integrated and working
- Customizing the Dashboard, reports and views as requested by RSCL (Example customizing reports related to eChallan, Traffic Violation, attending waste bins by the waste collection vehicles etc.., and bringing them over the dashboard).
- Adding new SOP's to the ICCC library and customizing the same as per RSCL's request.

Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, up-gradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements, preventive and corrective maintenance of the smart city ICT components deployed as part of this project and shall maintain service levels as defined in the RFQ cum RFP. All equipment and material supplied by the MSI shall be provided with standard warranty against defects of design and

manufacturing and against faults and failures associated with workmanship of MSI and its sub- contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the Client.

MSI shall provide all the technical, managerial, and other staffing required to manage day-to- day maintenance of the smart city ICT components during the Contract period, including different categories of resources (L1, L2 or L3) for managing the ICCC and DC as per SLAs.

All spares required for the smooth operation of the smart city ICT components shall be maintained by the MSI for the entire duration of the contract to meet SLA requirements. The cost of the spares, repairs, and replacement shall all be deemed to be included in the price quoted by the MSI. MSI shall also institutionalize structures, processes and reports for management of SLA. Root cause analysis and long term problem solutions shall also be part of MSI scope.

MSI shall maintain all data regarding entitlement for any update, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the Client during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any changes to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system. Issue log for errors and bugs identified in the solution and any change done in solution shall be periodically submitted to the Client.

MSI shall ensure OEM support during Comprehensive Maintenance stage for system performance, performance tuning, updates etc. MSI shall provide all support for formulation of all policies and procedures related to System Administration, Data Base Management, applications, archives, network management & security, back up and data recovery and archive, data synchronization after crash.
MSI shall prepare a detailed System administration manual, Data administration manual, operational manual, User manual which shall be used by Client's employees to operate smart city ICT components. This shall also include how the various parameters shall be monitored/ tuned in a live system. Preparation of requisite system configuration for disaster recovery management and fail over system plan shall also be under the supervision of MSI. The MSI shall also maintain the following minimum documents with respect to ICT components:

- High level design of system
- Module level design of system
- System Requirement Specifications (SRS)
- Any other explanatory notes about system
- Traceability matrix
- Compilation environment

MSI shall also ensure updation of following documentation of software system:

- Documentation of source code
- Documentation of functional specifications
- Application documentation is update to reflect on-going maintenance an enhancement including FRS and SRS, in accordance with the defined standards
- User manuals and training manuals are updated to reflect on-going changes/enhancements
- Adoption of standard practices in regards to version control and management

The communication costs (Internet charges, telephone charges, 3G/GPRS connectivity charges) and any other incidental charges related to maintenance period shall be in the scope of the MSI and considered to be included in the proposal submitted by the MSI for the entire contract duration.
Any planned and emergency changes to any component during maintenance period shall be through a change management process. For any change, MSI shall ensure:

- Detailed impact analysis

- Change plan with roll back plan
- Appropriate communication on change required has taken place
- Approvals on change
- Schedules have been adjusted to minimum impact on production environment
- All associated documentation are updated post stabilization of the change
- Version control maintained for software

Any software changes required due to problems/bugs in the developed software/application will not be considered under change control. The MSI will have to modify the software/application free of cost. This may lead to enhancements/customizations and the same needs to be implemented by the MSI at no extra cost.

If the Operating System or additional copies of Operating System are required to be installed/ reinstalled / de-installed, the same should be done as part of the post implementation support.

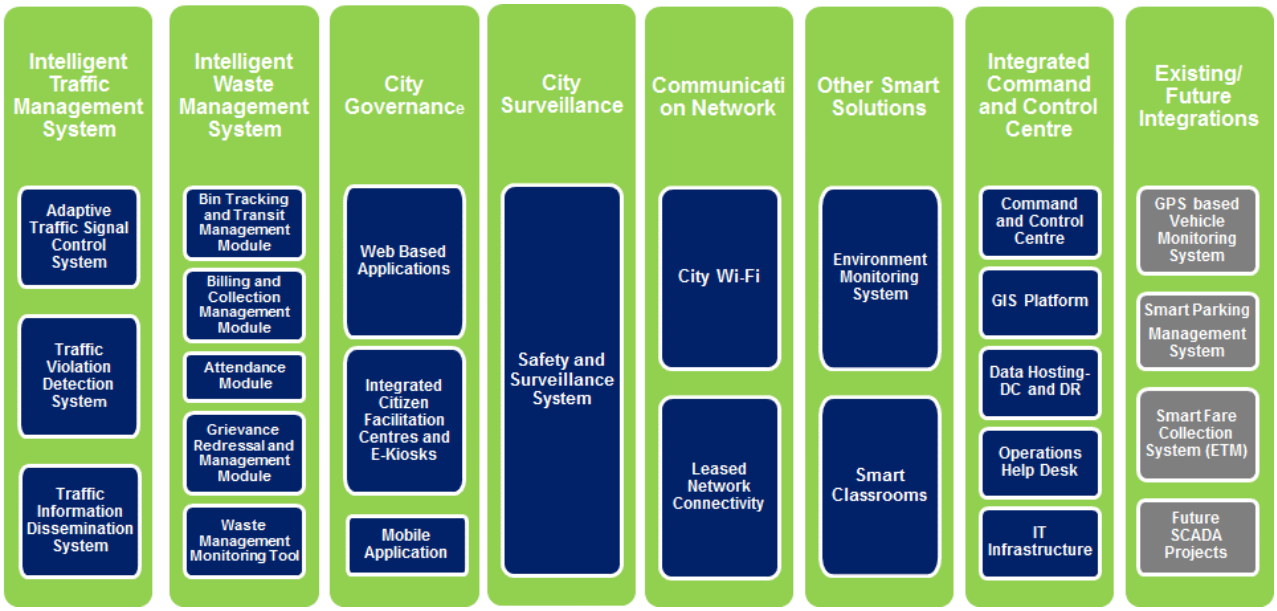
MSI shall also provide operations support for (Not limited to):

- Data Backup/Archival over tape drive/ other means agreed as per solution design
  - For RLVD/Traffic videos/evidence as per RSCL requirement.
  - eChallan data archival as per RSCL specified frequency.
  - Data archival policy specified as per eGov standards
  - Video stream to be archived post 30 days
- Retrieval of the Backup/Archival data from tape drive/ other means agreed as per solution design

Key Modules and Overall Requirements

Key Modules

Key modules to be implemented as part of the smart city solution is depicted below:



Integrated Command and Control Center (ICCC)

The Integrated Command and Control Center will receive input from different sources and field devices installed as part of waste management, traffic management, safety and surveillance, environment etc. Feeds from these sources will be assimilated, analysed and visualized over single platform resulting in an aggregated city level information providing integrated single view to city operators. Further, this aggregated city level information could be converted to actionable intelligence, which would be transmitted to relevant stakeholders and citizens for appropriate responses and information.

Data Center and Disaster Recovery Center

The Data Centre will house the application and storage servers in the required secured environment. The Data Centre will be co-located at the site identified for the ICCC. The Disaster Recovery Centre is proposed at Bhubaneswar, which falls under a different seismic zone.

Network connectivity on Lease

The MSI shall in consultation with RSCL select a telecom operator who can provide the requisite city network backbone infrastructure that will enable connectivity across all field devices, sensors, ICCC and DC & DR on lease basis

Intelligent Traffic Management System

The Intelligent Traffic Management System (ITMS) aims at improving the efficiency and effectiveness of the traffic management system through centralized monitoring and management at the ICCC. ITMS related solutions will focus on implementation of a Adaptive Traffic Control System, Traffic Violations and Detection System (based on ANPR) with E-Challan capturing Red light violations, Zebra crossing violations, Speed violations, Free left violations as well as wrong direction movement.

Intelligent Waste Management System

The Intelligent Waste Management System aims to streamline the overall process of solid and liquid waste management including secondary collection of solid waste at garbage depots, waste transportation by waste

collection and cesspool vehicles to the landfill/septage treatment plant site, attendance of the field staff, billing and collection, etc.

City Governance

The overall objective of this module is to improve interaction between the city administration and residents and other city dwellers, with an overarching objective of making urban services more accessible for all providing access through multiple channels e.g., web platform, citizen facilitation centers, e-Kiosks, Mobile Application, etc.

Safety and Surveillance

The core objective is to create a supporting mechanism for the city law enforcement agencies through 24x7 surveillance and monitoring throughout the city as well as enable proactive identification of security issues leveraging intelligent analytics from the surveillance system. This module proposes implementation of a holistic safety & surveillance system across the city including:

- Installation of PTZ and Fixed cameras with video analytics, edge analytics capabilities in 110 locations
- Develop a full fledged command and control for ensuring 24X7 monitoring and enabling effective action to be taken in case of law and order/ disaster situations
- Integration with existing safety & surveillance systems already implemented as part of the initiative taken by SP Office. etc.

Other Smart Solutions

1. **Public Address System**
   Public Address (PA) system shall be used at intersections, public places, market places and other strategic locations as identified by RMC to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. This system shall be used to announce informatory and emergency messages to the road users and will be connected to the ICCC system application. The PAS System shall be capable of playing pre-defined audible messages from the ICCC.

2. **Variable Messaging Signboards**
   Variable messaging displays will be setup across the city and will be used to display information related to traffic congestion, accident, disruptive incidents, ongoing roadwork zones, speed limits & traffic diversions, key notices or messages from RMC like information about any emergency or disaster, etc.

3. **Environment Monitoring System**
   Environment monitoring system monitors the real time information on air quality parameters recorded using environmental sensors on a regular basis and help in reducing the pollution level in the city. Information captured by sensors shall be fed into the System software which shall process the data using analytics at ICCC and the result shall be displayed in the Digital Display screen installed at strategic locations.

4. **Wi-Fi Hotspots**
   Wi-Fi hotspots are proposed to be installed to enable citizens to collaborate and perform business activities with a high speed and seamless network connectivity. This connectivity will be highly secure via user authentication mechanism and chargeable beyond free data limits. There will be Wi-Fi controller which will monitor, manage, and control access points from the ICCC. Wi-Fi access points shall provide low cost, secure connectivity for IoT applications, smart buildings and city administration.

5. **Smart Classrooms**
   Smart Classroom envisages to provide quality education to students using digital educational content delivered through projectors and smart boards to the students of Government Schools together with surveillance to ensure monitoring of Smart Classes.

6. **Artificial Intelligence, Machine Learning and Edge Analytics**
   All Cameras should be enabled to run analytics on all the use cases leveraging artificial intelligence on all the edge device and must show continuous improvement during operations. All use cases should be demonstrable at individual sensors/devices at all locations.

Integration Requirements

Integration services shall include:

- Set-up data movement for various systems under integration framework;
- Create enterprise integration framework for various integration touchpoints. Approach for integration shall be SOA based and must be facilitated by industry best practices;
- Validation of data movement between source and target system.

MSI is required to propose a composite solution for integration which is SOA (Service Oriented Architecture) and Business Process Management (BPM) enabled. The solution will be configured to meet the requirements of workflow processes across systems. The integration between systems will be based on Open API standards. The proposed solution shall

- Offer highly secured means of integration with existing applications
- Support encrypted and secured means data exchange
- Maintain complete audit trail and logging of data exchanged

The integration scope is divided into 3 types

- Existing applications
- New applications that are part of this RFP
- Future Integration

The table below provide indicative list of systems that has to be integrated with ICCC and brief scope of work:

No.	Service	Brief Scope of Integration (Existing/New)
1.	Waste Management	• ICCC shall be integrated with the Intelligent Waste Management system for real time tracking of waste, cesspool vehicles and bins, raising billing and collection, monitoring attendance and addressing grievance redressal, etc.
2.	Traffic Management	• ICCC shall integrate with Intelligent Traffic Management System comprising Adaptive Traffic Signal Control System (ATCS), Traffic Enforcement System including traffic violation detection, E-challan, etc. using Automatic number plate recognition
3.	City Governance	• ICCC shall be integrated with exisiting applications and the Integrated Business Process Management Services solution for online delivery of citizen services, including grievance redressal provided by RMC, RDA, PHEO, etc. through smart city app, CFCs/e-kiosks, etc.; incidence/ emergency response management system like police, ambulance, fire, etc.
4.	City Surveillance	• Surveillance system shall be integrated with ICCC to ensure safety and security of the citizens across strategic locations in the city. • The safety and surveillance solution shall also be able to share the feeds, data to existing Police Command and Control Center
5.	Smart Wi-Fi	• ICCC will be required to integrate with Wi-Fi Hotspots sub System using Open API standards to receive the feeds related to - Wi-Fi status across city - KPI's related to free Wi-Fi • ICCC should be able to map this information on the GIS layer and help authority monitor the Wi-Fi Hotspots across the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective sub system. • All the information received from Wi-Fi Hotspots sub system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard.

No.	Service	Brief Scope of Integration (Existing/New)
6.	VaMS / PAS	• ICCC shall be integrated with Traffic Information Dissemination System comprising Variable Message Signboards (VaMS) and Public Address System (PAS)
7.	Environment Monitoring System (EMS)	• ICCC shall be integrated with environment sensors for monitoring of environmental parameters • The EMS outputs on various parameters shall be displayed through Digital Display Screens across strategic locations
8.	Smart Classroom	• Integration of CCTV surveillance of Smart Classrooms for monitoring
9.	Online GIS Platform	• Completely integrated for all City Applications and Services. The GIS Platform shall act as the single unified data map for Rourkela. The Data collected/generated for the maps shall be available to all application/agencies from time to time.
Future Integration		
10.	All existing/future solutions related to transportation, smart parking, as well as all future constructions, viz. water supply, sewerage, etc. with ICT components (e.g. SCADA system) shall be integrated with the IoT platform at the Integrated Command and Control Center/ Data Center.	

Responsibility of MSI

The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The MSI is free to offer products and solutions, which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an Optimized solution, which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

Standards and Protocols

The MSI solution shall comply with the following standards as well as others as may be applicable:

S.No.	Standard/Protocol	Remarks
1.	Biometrics Standard	http://egovstandards.gov.in/notified-standards-0
2.	Digital Preservation Standards	http://www.egovstandards.gov.in/guidelines-0
3.	Localisation and Language Technology Standards	Unicode Standards 5.1.0 and future upgrades, ISO/IEC 14496-OFF
4.	Copy Right	Proper copyright policy
5.	Use of National Emblem	Directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.
6.	Domain name convention	Government's Domain Name Policy
7.	Link with National Portal	As per guidelines provided in at http://india.gov.in/linktous.php
8.	Content Hyper linking	Hyperlinking Policy
9.	Metadata and Data Standards	http://egovstandards.gov.in/notified-standards-0
10.	Mobile Governance	http://www.egovstandards.gov.in/guidelines-0

S.No.	Standard/Protocol	Remarks
11.	Guidelines for Indian Government Websites	http://www.egovstandards.gov.in/guidelines-0
12.	Open APIs/Open Standards like One M2M	http://egovstandards.gov.in/frameworkinstitutional-mechanism-and-policies
13.	Internet of Things	• Sensors & Actuators (IEEE 1451) • Identification technology (ISO/IEC JTC 1/SC 31) • Domain Specific Compliance-respective domain specific standards like HL 7 for healthcare devices etc.
14.	Communication Technology	Thread, AllJoyn, IEEE 802.15.4, IETF 6 LoWPAN, IETFROLL, IETF CoAP
15.	Use Case/Application Specific	Domain specific standards like IEEE 11073 for e-health etc.
16.	Consortia	Open Interconnect consortium, Industrial Internet Consortium
17.	Architecture Technology	IEEE P2413
18.	Disaster Management	Please refer Annexure B
19.	Cyber Security	Cyber Security Model Framework for Smart Cities vide Ministry of Housing and Urban Affairs (erstwhile Ministry of Urban Development), Government of India OM No. K-15016/61/2016 SC-1 dated 20th May 2016
20.	Information Security	ISO 27001
21.	IT Infrastructure Management	ITIL specifications
22.	Service Management	ISO 2000 specifications
23.	Project Documentation	IEEE/ISO/CMMi
24.	Differently abled people	Should be compliant with The Rights of Persons with Disabilities Act, 2016 and related guidelines.

Integrated Command and Control Centre

Objective

To enhance the safety and security, improve efficiency of city administration and ensure better quality of life for residents, Rourkela intends to develop a robust ICT infrastructure that supports digital applications and ensures seamless steady state operations, traffic management, emergency response mechanisms and real time tracking of services and vital city metrics throughout the city.

The ICT infrastructure setup shall be monitored through the Integrated Command and Control Centre (ICCC) which will serve as the 'nerve centre' of Rourkela and assist in enhancing efficiencies of city operations and management. It shall provide a holistic view of all city operations allowing monitoring, control and automation of various functionalities at an individual system level along with enabling cross-system analytics. The ICCC shall be deployed in Rourkela as part of this project, to make the city operations intelligent, integrated and efficient.

ICCC is envisioned to provide an integrated platform enabling (a) sharing of real-time information amongst various departments and (b) evidence based decision making thereby improving the efficiency of the city administration and improving quality of life of the citizens.

ICCC enables collation of information and collaborative monitoring, thus helping in the analysis of data for quicker decision making. Intelligent operations capability ensures integrated data visualisation, real-time collaboration and deep analytics that can help different stakeholders prepare for exigencies, coordinate and manage response efforts, and enhance the ongoing efficiency of city operations. Key benefits accruing from the ICCC are as follows:

- Shall enable cross-system and cross-agency coordination to monitor, operate and manage the city in an integrated manner.
- ICCC platform shall enable different agencies and departments of Rourkela to monitor and utilize information of other departments for delivering services in an integrated and more efficient manner.
- ICCC shall be able to normalize the data coming from different devices of various Original Equipment Manufacturers (OEMs) leveraging the IoT platform. It shall support integration with multiple vendors.
- ICCC platform shall enable various visualization and analytics of city operations to improve decision making. These analytics shall be achieved via cross-system integration of various systems and as per the standard operating procedure. Analytics shall include both prescriptive and predictive analytics.
- ICCC shall provide reporting capabilities for city administrators to keep record of city operations.
- The systems at ICCC shall ensure that integrity and confidentiality of all information gained is secure at all times.
- The ICCC platform shall be the integration point at which data from across the city converges for processing. This shall allow all information to be managed within the same network, eliminating many communication problems that are faced by working in silos.
- The ICCC shall be rated for 24x7 operations and shall provide shift based operations for an overall 24x7 support.
- ICCC platform may not necessarily duplicate all functionality derived out of individual system specific applications but will monitor and integrate various features using which an intelligent city operation can be achieved.

Scope of Work

The MSI shall ensure successful implementation of the proposed ICCC as per the scope of services described below

- **Waste Management:** ICCC shall be integrated with the Waste Management system for real time tracking of solid waste vehicles, cesspool vehicles and bins, raising billing and collection, monitoring attendance and addressing grievance redressal, etc.
- **Traffic Management:** ICCC shall integrate with Intelligent Traffic Management System comprising Adaptive Traffic Signal Control System (ATCS), Traffic Enforcement System including traffic violation detection, E-challan, etc. using automatic number plate recognition.

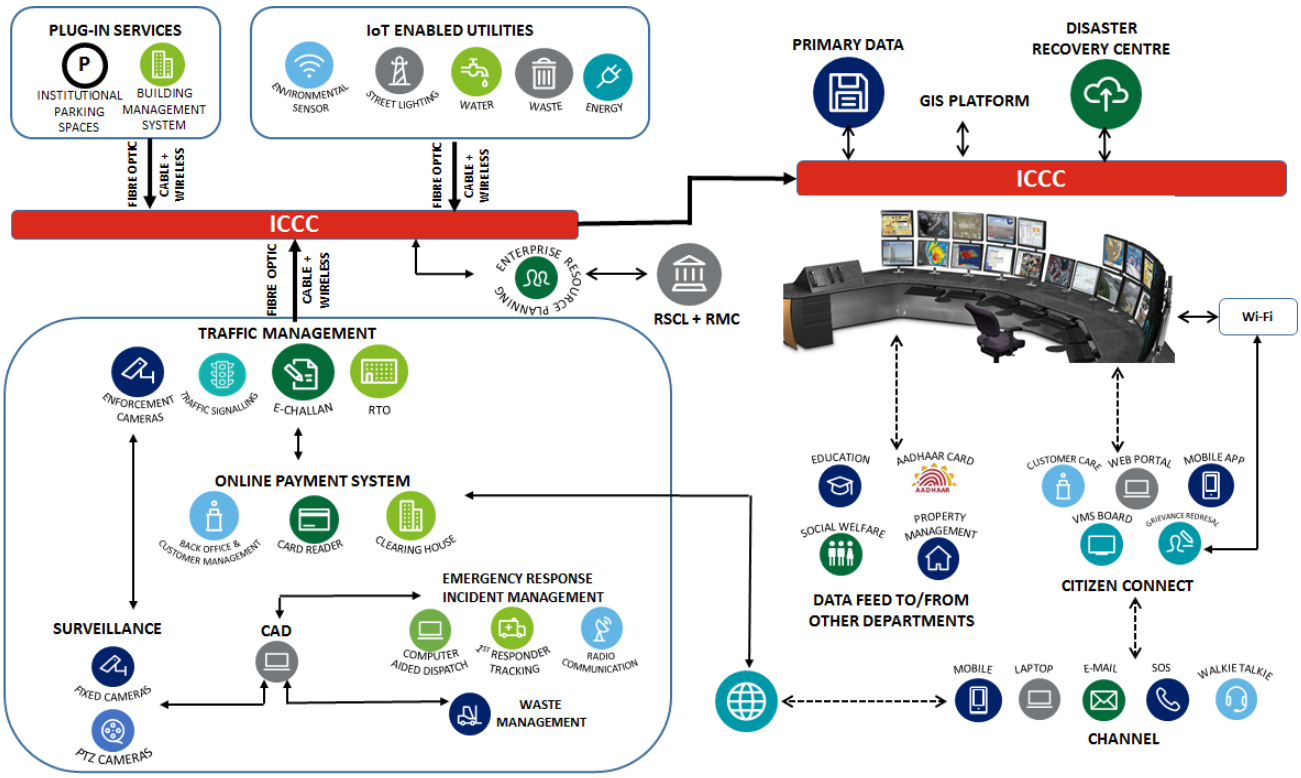
- **City Surveillance:** Surveillance system shall be integrated with ICCC to ensure safety and security of the citizens across strategic locations in the city.
- **City Governance:** ICCC shall be integrated with e-municipality for online delivery of citizen services, including grievance redressal provided by RMC, RDA, PHEO, etc. through smart city app, CFCs/e-kiosks, etc.; incidence/ emergency response management system like police, ambulance, fire, etc., air quality monitoring system, SCADA system, etc.
- **VaMS / PAS:** ICCC shall be integrated with Traffic Information Dissemination System comprising Variable Message Signboards (VaMS) and Public Address System (PAS)
- **Environment Monitoring System (EMS):** ICCC shall be integrated with environment sensors for monitoring of environmental parameters. The EMS outputs on various parameters shall be displayed through VaMS
- **Online GIS Platform:** Completely integrated for all City Applications and Services. The GIS Platform shall act as the single unified data map for Rourkela. The Data collected/generated for the maps shall be available to all application/agencies from time to time.

In addition to the applications highlighted above, the ICCC shall enable seamless integration with applications to be deployed in future through ensuring open API standards.

The functional requirements and technical specifications provided in the below sections are indicative and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

Indicative Solution Architecture

The indicative architecture for the proposed Integrated Command and Control Center has been depicted below:



The Pan City Proposal of Rourkela Smart City consists of various components which is illustrated in figure above. The components are namely:

- Waste Management system
- Traffic Management System
- City Governance including e-Governance, Citizen Facilitation Centers, e-Kiosks, Mobile App
- Safety and Surveillance System
- City Wi-Fi
- Environment Monitoring System
- Smart Classroom
- Central Command and Control Centre

As per the Pan City Proposal, the Central Control Centre is planned to be an Integrated Command and Control Center (ICCC) that will integrate all the pan city components and city services.

Minimum Functional Requirements

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/1.01	Solution & Platform	• Should have built-in fault tolerance, load balancing and high availability & should be certified by the OEM. • Software (Application, Database and any other) should not be restricted by the license terms of the OEM to prevent future scaling up • System should provide a comprehensive API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration with existing systems, and future application and sensors which will be deployed on the field. • The solution should be network and protocol agonistic and provide option to connect legacy system through API's with either read, write or both options. It should connect diverse on premise and/or cloud platform's and makes it easy to exchange data and services between them. • The system shall allow seamless integration with all of the department's existing and future initiatives • The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. • The Command & Control solution should be implemented and compliant to open standards based Commercial-of the-shelf (COTS) products India. • The platform should be able to normalize the data coming from different field devices or other existing or to be integrated applications and enable use of these data seamlessly across different interfaces.	
ICCC/FR/2.01	Convergence of Multiple feeds / services	• System need to have provision for interfacing with various services and be able to monitor them. The solution should integrate existing deployed solution by City and also need to provide scalability option to implement new use cases. • System should have capability to source data from various systems implemented in Rourkela city (implemented as part of this project or other future projects) to create actionable information.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/3.01	Standards for ICCC Application Software	• The solution should adhere to the Industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility. • Compliant to IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management • Compliant to Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring. • Compliant to Geo Spatial Standards like GML & KML etc.	
ICCC/FR/4.01	ICCC Application Software Components	• Web server to manage client requests to provide web-based, one- stop portals to event information, overall status, and details. The user interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards. • Application server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases, and files (Both structured and un-structured) It should provide business monitoring service to monitor incoming data records to generate key performance indicators. It should also enable users to view key performance indicators, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. The application server should provide security services that ensure only authorized users and authorized groups can access data. Analytics functionality can be part of application server or a separate server	
ICCC/FR/5.01	Incident Management System	• The system should provide Incident Management Services to facilitate the management of response and recovery operations • Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds. • Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention. • Should support for multiple incidents with both segregated and/or overlapping management and response teams. • Should support Geospatial rendering of event and incident information using relevant GIS services and GIS Servers • Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps. • Should support incorporation of resource database for mobilizing the resources for response. • Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		be captured in standard formats to facilitate incident correlation and reporting. • The system should identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems • Should provide detailed reports and summary views to multiple users based on their roles. • A Reference Section in the tool should be provided for posting, updating and disseminating plans, procedures, checklists and other related information. • Provide User-defined forms as well as Standard Incident Command Forms for incident management.	
ICCC/FR/6.01	Integration with Social Media & Open Source Intelligence	• Should provide integration of the Incident Management application with the social media. • Should provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground. • Should extract messages and display it in an operational dashboard. • Should have ability of scenario reconstruction • Should be able to correlate the extracted message from the social media with existing other events and then should be able to initiate a SOP. • Should be able to take action directly to sensor execution based on requirement. • Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started. • Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.	
ICCC/FR/7.01	Integrated User Specific & Customizable Dashboard	• Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance • Collects major information from other integrated City sensors/platforms. • Should allow different inputs beyond cameras, such as PC screen, web page, and other external devices for rich screen layout • Multi-displays configurations • Use of GIS tool which allows easy map editing for wide area monitoring (Compatible with Google map, Bing map, ESRI Arc GIS map, open GIS etc.). • Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command center • Should provide real time and historical reports, event data & activity log. The reports can be exported to pdf or html formats. • Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, incident types, event titles and stakeholders involved , etc. and capability to drill down to the details	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/8.01	Device Status, Obstruction Detection and Availability Notification	• Should provide icon based user interface on the GIS map to report non- functional device. • Should also provide a single tabular view to list all devices along with their availability status in real time. • Should provide User Interface to publish messages to multiple devices at the same time.	
ICCC/FR/9.01	Event Correlation	• ICCC Application Software should be able to view two or more events coming from different subsystems (incoming sensors) based on time, place, and custom attribute and provide notifications to the operators. The ICCC shall be able to get, capture, record incidents occurring in real time from all possible sources and to channelize the data and processed outcome to respective connected application (MSI / Departmental / Other Government - provided application both for current use like in video wall displays and in other historical analytics.) Such notifications will be triggered by the events captured in the downstream (south bound) applications that are integrated to the command center through APIs.	
ICCC/FR/10.01	Standard Operating Procedures (SOPs)	• The platform should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface. • Users should be able to edit the SOP, including adding, editing, or deleting activities based on their respective roles (Role Based Access). • Users should be able to also add comments to or stop the SOP (prior to completion). • There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review. • SOP Tool should have capability to define the following activity types: • Manual Activity - An activity that is done manually by the owner and provide details in the description field. • Automation Activity - An activity that initiates and tracks a work flow and select a predefined flow order from the list. • If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else. Shall use inputs from related other devices to auto-configure responses and email responses to relevant stakeholders creating both time stamped event response and the actual communication sent out to the Smart City administrative hierarchy and to the field formations • Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification as per manual alternate responses to the situation, if not an automated standard response to the Smart City administrative hierarchy and the field formations	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• SOP Activity - An activity that launches another standard operating procedure.	
ICCC/FR/11.01	Instant Messaging	• Provide ability to converse virtually through the exchange of text, audio, and/or video based information in real time with one or more individuals within the emergency management Community.	
ICCC/FR/12.01	Actions Module	• ICCC Application Software should provide for authoring and invoking un-limited number of configurable and customizable actions through graphical, easy to use tooling interface. Such actions will be defined for each downstream (south bound) applications through a requirements gathering and pre-configuration process with user departments. • The users should be able to edit the action plan, including adding, editing, or deleting the activities with role based access. • The users should be able to also add comments to or stop the action plan as per role based authorizations and approvals. • There should be provision for logging the actions so that an electronic record is available for after-action review. • The tool should have capability to define the following activity types: - Manual Activity - An activity that is done manually by the owner and provide details in the description field. - Notification Activity - An activity that displays a notification window that sends out an auto email and SMS to concerned hierarchical stakeholders and may contain an email template for the activity owner to complete additional action items, and then sends a further email notification and a SMS.	
ICCC/FR/13.01	Key Performance Indicator	• ICCC Application Software should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies based on the real time responses that were enabled and the duration by which normalcy was restored, the stake holders who were involved and acted upon in the event and the outcome recordings of the Admin hierarchy on closure of the event etc. . • Indicators that the status is acceptable, based on the parameters for that KPI, no action is required. • Indicators that caution or monitoring is required, action may be required. • Indicators that the status is critical and action is recommended.	
ICCC/FR/14.01	Reporting Requirements	• ICCC Application Software should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators	
ICCC/FR/15.01	Collaboration Tools	• Should provide tools for users to collaborate in real-time using instant messaging features. • Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries, during emergency. • Provide the capability to invite - Using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information. • Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, and E-mail.	
ICCC/FR/16.01	Authentication	• User authentication information to authenticate individuals and/or assign roles.as and when required and it should be configurable as per requirement without any additional module	
ICCC/FR/17.01	Events Display Events and Directives control	• Should provide the capability for the events that are produced from a sub- system and are forwarded to the ICCC Application Software. Events could be a single system occurrence or complex events that are emanating from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the Command & Control Centre, the event should be displayed on an operations dashboard and analyzed to determine a proper directive. • Directives issued by the Command and Communications Center should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.	
ICCC/FR/18.01	What-if Analysis Tool	• The solution should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery. • To take proactive decisions that help minimize risks and damages, the solution should provide Analytical and Simulation systems as part of the Decision Support System. The solution should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy to use Graphical User Interface. When in What-If Analysis mode the solution should highlight not only the primary asset impacted but also highlight the linked assets	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		which will be impacted. The user should be able to run the What-if Analysis mode for multiple types of emergency events such as Bomb Blast, Weather events, Accidents etc.	
ICCC/FR/19.01	Alert & Mass Notification Requirements	• The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media. • Provide function for creating the alert content and disseminating to end users. Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service. • Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.	
ICCC/FR/20.01	Security & Access Control	• Provide comprehensive protection of web content and applications on back- end application servers, by performing authentication, credential creation and authorization.	
ICCC/FR/21.01	Internet Security	• Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central repository for administration purposes.	
ICCC/FR/22.01	Access and Permission	• Should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely	
ICCC/FR/23.01	User group	• Provide policies using separate dimensions of authorization criteria like Traditional static Access Control Lists that describe the principals (users and groups) access to resource and the permissions each of these principals possess.	
ICCC/FR/24.01	Provide multi-dimensional access control	• SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.	
ICCC/FR/25.01	Flexible single sign-on (SSO)	• Support LDAP authentication mechanism	
ICCC/FR/26.01	Authentication	• Should have ability to respond to authentication of users and end points	
ICCC/FR/27.01	Situational Awareness COP (Common Operational Picture)	Should be able to combine data from various sources and present it as different views tailored to different operator's needs and comprise of a comprehensive view of the events as on a specific date and time which should include but not be limited to the following: • Manual tasks assignment and their status • Agencies involved • Resources deployed • Timeline view of the situation	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/28.01	Timeline and Charting	• Event information • Resources information • Agency type • Tasks • Criticality or priority	
ICCC/FR/29.01	GIS Integration	• Shall view the environment through geospatial or Dynamic computer- generated (JPEG, BMP, AutoCAD, etc.) reusable map. • Should allow user to view sensor or system data and related name from the displayed map • Should allow all resources, objects, sensors and elements on the map to be georeferenced such that they have a real world coordinate. • Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle. • Should visually display an alarm generating sensor on map. • Should visually differentiate sensor alarm severities on map through different color and icon identifiers. • Should immediately view alarm details (including description, video, etc.) and investigate the alarm from the map. • Should allow user to choose camera and other sensors from map to view live video and the data. Where shared feed is provided, ability to zoom in using the selected camera for dynamic real time image focus and capture and use feature is required • Should allow user to choose camera and take live video image snapshot and save to file from any camera. • Should allow user to choose camera from map to move PTZ cameras and play, pause, stop, fast-forward, rewind, and play recorded video from pre-set time. • Should allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video should allow user to jump from one map to the next with a single click of a mouse with map web based links. • Should allow map information “layers” to be displayed/hidden on items such as - Sensor names - Sensors - Sensor range (e.g. camera – orientation, range, field of view angle) - Locations and zones - Perimeter range - Resource tracks - Allow user to zoom in/out on different regions of map - Graphic	
ICCC/FR/30.01	Video Display	• Shall view live or recorded video from resizable and movable windows • Should have an intuitive built-in video redaction module allows users without advanced video editing knowledge	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		to spend less time when redacting video, while also ensuring accurate results are maintained. • Should have an ability to perform video controls for video systems from workstation • Shall play, fast-forward, rewind, pause, and specify time to play recorded video • Shall take a video still image (snapshot) from live or recorded video • Shall export video for user specified time and duration in standard formats (like mp4, etc.) • Shall have the capability to move PTZ cameras as well as zoom-focus on non-PTZ cameras with digital magnification and object filter etc., for view clarity • Shall view Video in Video Matrix • Shall display in 1x1, 2x2, and 3x3 window formats or any other formats as determined by RSCL based on current and future sizing of video wall • Shall enable operator to specify video windows to be displayed in matrix • Shall enable matrix settings to be saved per user • Shall view either live or recorded video can be displayed in the video matrix window. • Shall enable video snapshot to be taken and saved from any window pane in the matrix view • Shall rotate video in “virtual” video guard tour • Shall rotate through multiple video views based on predefined video camera sequence and duration. • Shall enable the user to pause the rotation of video and resume the video rotation again • Shall enable times between new video to be adjusted • Shall enable both live video and recorded video to be played through the video guard tour. • Shall enable alarms to be generated from any video pane • Shall enable user to only view and control video for which they have been assigned permissions by the administrator • Shall have capability of manually create an alarm from the live or recorded video with specified severity and description	
ICCC/FR/31.01	Alarm Display	• Should have an ability to display alarm condition through visual display and audible tone • Should have an ability to simultaneously handle multiple alarms from multiple workstations • Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc. • Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence	
ICCC/FR/32.01	Historical Alarm Handling	• Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed. • Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/33.01	Alarm Reporting	• Should have an ability to generate a full incident report of the alarm being generated. • Should have an ability to display report on monitor and print report • Should have details of alarm including • severity, time/date, description and location captured video image snapshots • Relevant sensor data such as SCADA sensors • Response instructions • Alarm activities (audit trail) • Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and mht formats • Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location	
ICCC/FR/34.01	Alarm Configurations	• The solution should have the following ability to handle the workflow alarms through graphical user interface. Should have an ability to match keywords or text from the alarming subsystem's description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.) Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times. Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times should have an ability to assign specific actions for each alarm should have an ability to activate or deactivate alarms as required should have an ability to create exceptions should check and rectify logical errors and contradictory rules while creating exception rules should have an ability to schedule execution of rules should suspend or terminate the application of rule should archive unused or deactivated rules	
ICCC/FR/35.01	Rule Engine & Optimization	• Should have ability to respond to real-time data with intelligent & automated decisions • Should provide an environment for designing, developing, and deploying business rule applications and event applications • The ability to deal with change in operational systems is directly related to the decisions that operators are able to make • Should have at-least two complementary decision management strategies: business rules and event rules. • Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships	
ICCC/FR/36.01	System Functionalities and Resiliency	• System should support standard Authentication and Authorization for access.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Architecture should provide appropriate resiliency for the system to ensure high availability and trouble free operations. • The High Availability should be for all the components of ICCC. • Ensure ways and means to define policies that make applications or objects respond to various external eco system. • Provide Scheduler for future actions. • Should have integrated collaboration tools to bring multiple stake holders and responders to respond an emergency or an urban services event. • Should provide different tier of user categorization, authentication, authorization, and services. • Should provide role-based access view to applications. • Ensuring time shifted and real-time data (structured and unstructured) available for big data and analytics using Integrated analytics platform (with ETL (Extraction, Transformation and Loading), Integration, Modelling & Simulation, Dash boarding). • Should also be able to ingest other utilities, ERP, e-governance data • OEM should be able to securely access the system remotely for updates / upgrades and maintenance for the given duration. • The system should be able to be deployed across multiple sites and on cloud for operations and disaster recovery purposes.	
ICCC/FR/37.01	Edge Devices & Application Gateways	• Provides standard appliance or software or hardware combination to connect IoT devices / applications, provide secure connection to IT infrastructure, provide remote lifecycle management including software/firmware downloads and upgrades/updates, provides remote management, self-registration, and local administrative interface. • Gateways to provide software modules to interact with control systems and protocols. • Provide centralized Device Management from sensor to the IT setup. • Provide management tools to view, analyses, report on and modify the device configurations. • Gateway software should be agnostic to sensors and devices protocols.	
ICCC/FR/40.01	API Management and Big Data Analytics	• Availability of vendor/platform agnostic APIs to control all IOT functionality. • Access to the platform API(s) should be secured using API keys. • Relevant and appropriate APIs should be made available for all the listed IOT domains to monitor, control sensor and/or actuators functionality to enable sensor vendors and app developers to develop apps and connectors / adaptors to the platforms. • APIs enabling contextual information and correlation across domains and verticals for multiple platforms and multiple sensors, as and when needed in future.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Availability of vendor/platform agnostic APIs to control all IOT functionality. • Should have ability to run Descriptive, Predictive, Prescriptive and cognitive analytics by using of scenario reconstruction ability.	
ICCC/FR/41.01	Events & Policies Management	• System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should be a set of conditions that activate the behavior it provides. • System should allow Default, Time-based, Event-based and Manual override polices creation. • System should provision to define a set of conditions that can be used to trigger an event-based policy along with correlations	
ICCC/FR/42.01	Notifications, Alerts and Alarms	• System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Field Responder Mobile App if required. • All system messages (notifications, alerts and alarms) should always be visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays. • Systems should deliver message to a set of users. The Notification service should support notification methods such as Email and SMS.	
ICCC/FR/43.01	Users and Roles	• Platform should allow different roles to be created and assign those roles to different access control policies. Based on their roles and the permissions, they should be allowed to perform various tasks, such as adding new locations, configuring new devices, managing adapters etc. • Platform should allow single or multiple users to view and manage alarms in defined domains (areas/locations). User thus can be part of single or multiple domains. • The platform shall be available with unlimited number of user license (perpetual) for viewing and access across multiple departments, administrators and operators, as and when required without any license restriction on concurrency of number of simultaneous users.	
ICCC/FR/44.01	Dashboard	• Platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. The Smart City dashboard shall also connect seamlessly to any state level dashboard view of identified and authorized other systems like CM Dashboard etc. • System should provide trends in graphical representation from data sources over a period. Trends should allow to monitor and analyses the event details w.r.t. time and also device performance over time with the help of third party device monitoring tools. • Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/45.01	Reports	• System should have ability to generate reports and have provision to create user specific standard list of reports. • Should provide historical reports, event data and activity logs. The reports can be exported to PDF or HTML formats. • Ability to display report on monitor / video wall and print report. • Ability to capture Operators response. • Ability to select information and fields to be included in report at time of report generation. • Ability to generate details of alarm including severity, time / date, description, and location. • Ability to associate Map of surrounding area associated with alarm. • Allow operator to transfer the incident report to Mobile Device/another operator's console.	
ICCC/FR/46.01	Mobile Access for Field User	• The platform should provide Integrated Mobile Application for Android, Windows and iOS, for capturing real-time information from the field response team using Mobile Standard Operating Procedure. • Field Responder should be able to acknowledge the incident and provide real time updates from the incident site using approved and authorized mobile Apps and mobile interfaces to be provided by the MSI for use by the RMS / RDA / Government Official / Municipal School staffers / Parents of students of Municipal schools	
ICCC/FR/47.01	Additional Features and Licensing	• The Platform should account for below solution components, which can be extended to Multi-tenancy architecture: • The platform shall be available with unlimited number of user license for viewing and access across multiple departments, administrators and operators, as and when required without any licensing restriction on concurrency of number of simultaneous users. • License for integration of various sensors, applications/systems as per the quantities / counts of edge devices / sensors / applications.	
ICCC/FR/48.01	Data Integration and Advanced Analytics	• Able to integrate, connect, and correlate information from IoT platforms / applications, various edge/field devices and other IT & non-IT systems, providing rule based information drawn from various sub-systems for alert generations. • Should support on the fly deployment of Sensors/IoT Devices and shall have the ability to add / remove sensors including new OEM types without a need for shutdown. • Carry the ETL process and then normalize and integrate / ingest the data coming from different devices of same type and provide secure access to that data (both structured and unstructured) using data API(s), ESB etc. including the SCADA data, to application developers for various devices being used by the city for various urban services, monitoring, delivery or surveillance etc.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The Platform should be able to define its own data model for each urban service as needed for the city and map the data from different devices to the common data model, with the help of built-in modelling and simulation tools. This will enable avoiding the complexity of various data formats and carry advance data analytics from time to time to generate reports and create dashboards for various connected / inter-dependent city operations. • Data from the IoT / edge devices and applications should be exposed to application eco system using secure APIs using API keys or using ESB tools. • Attributes of API key(s) or ESB tools should restrict / allow access to relevant data based on various attributes, domains and tenants. • Should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used, agnostics to various sensor technologies and allow the sensor OEMs to develop integrations using SDKs, ESBs, Scripts, etc. without affecting the existing application and integration. • Should support distributed deployment of functions (workflows & policies) across city's infrastructure with centralized management and control.	
ICCC/FR/49.01	System Operations	• The platform should have built-in geospatial visualization layer compliant to industry open standard applications • The platform should provide operators and managers with a management dashboard that provides a real-time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. • The platform shall provide the day to day operations and situational awareness to the participating agencies during various modes of operation. • Shall provide a uniform, coherent, user-friendly and standardized interface. • Shall provide possibility to connect to workstations, video walls and accessible via web browser. • Dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard. • The platform should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes. • Shall be possible to combine the different views onto a single screen or a multi-monitor workstation or video walls. • Should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.\ • Audit trails should include detailed information about the user, activity type, date and time of addition/change/removal, and IP address accessed when the action occurred.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Should provide ability to extract data in desired formats for publishing, reporting and interfacing purposes. • Should provide ability to attach documents to incidents and other entities. • The platform is required to issue, log, track, manage and report all activities underway during the various modes of operation. • System should support centralized logging & auditing framework. • System should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs). • System should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, software licenses etc. • System shall provide integrated tool for evidence management of critical events and incidences digitally with provision for long term tamper proof data preservation so as to make it admissible in the court of law.	
ICCC/FR/50.01	Workflow Engine (WE)	• The ICCC should have the following Work Flow Engine Capabilities to integrate with any VMS to deal with any type of event data. • A Workflow Engine (WE) should be available to respond to any event data ingested as mentioned earlier	
ICCC/FR/50.02		The WE shall provide for dynamic camera(s) selection based on • Geo location of camera and event. • User definable ranges using user definable units of measure • Specific camera or sensor selection by external system	
ICCC/FR/50.03		The WE should provide for each user defined range, the following camera movement capability • Dynamic aim to event coordinates (without presets) • Move to the closest preset • Move to a specific preset • Start a specific tour • Snap camera to closest N,E,S,W direction after user defined delay • Zoom functions adjustable based on user defined scale and event type	
ICCC/FR/50.04		The WE should allow centralized user configurable actions by event and transaction types • Pop video to any VMS monitor / tile or any console • Generate a bookmark in the VMS • Generate VMS alarm • Generate a text message in the VMS • Send an e--mail message with snap shot • Send a SMS text message with snap shot to any phone • Control camera based on ranges • Execute a command	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Send a message to any VMS user or group of users • Play an audio file • Launch Internet Explorer to a URL in any VMS monitor / tile or console • Pop a map to any VMS monitor or any console tile • Add a user defined record to a user defined report • Display the event in a dynamic map along with all available camera locations	
ICCC/FR/50.05		The VSI should provide the ability to receive application events through all of the following mechanisms: • XML interface using user defined port and IP Address for each transaction type • Wait and listen for transactions • Initiate data request from external system • Email interface using any standard off the shelf e-mail system • Ability to develop custom interfaces as needed	
ICCC/FR/51.01	Analytics Engine: Threat level Indication	• Integrated City Operations Platform shall be integrated with analytics engine and which shall support following capability. • Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management. • Should support flexibility to integrate with other city and government software applications. • Analytics Engine module shall have below intelligence capabilities; • Advanced Predictive Analytics • Should predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc. • Support predictions with measurable accuracy of at least > 70% • Should predict and integrate with Smart City solutions helping in driving operational policies creation. • Should support a visualization platform to view historic analytics • The application should be able to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level system shall support following tasks: - Connect to a variety of data sources - Analyze the result set - Visualize the results - Predict outcomes • Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel, NoSQL, RDBMS, data from electronic records such as SMS, Emails etc. Evaluation of the system for selection shall also award suitable marks to each type of the above data handled in the system	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Analytics Engine should provide analysis of data from a selected data source(s). • Analysis enables to define arithmetic and aggregation operations that result in the desired output. • Analytics engine should provide capability to check analysis with multiple predictive algorithms	
ICCC/FR/51.02		**Analytics Engine Visualization:** • Analytics Engine should provide visualizations dashboard • In the visualization workspace, it should allow to change visual attributes of a graph. • User should not be allowed to alter the graph/visualization definition. • In the visualizations workspace, user should able to do the following operations: - Change the graph/visualization type - Print the graph - Export the graph - Narrow down on the value ranges - Toggle the axis labels - Integrate with other 3rd party applications seamlessly	
ICCC/FR/51.03		Analytics Engine module should have below intelligence capabilities: • Advanced Predictive Analytics and Correlation. • Flexibility to integrate and run analytics on various city utility and eGov / ERP applications and both structured and unstructured data sets. • The platform should be able to predict insights on data from various city IoT infrastructure and applications. • The platform should have predictions with measurable accuracy of at least 70% and improvise on a half yearly basis using machine learning on the data sets acquired over each half-year-period • The platform should be able to predict and integrate with Smart City solutions helping in driving operational policies creation. • Should provide integrated platform with end user access ranging from ETL, integration of data from structured & unstructured data sources, analytics with simulation and modelling and interactive dashboards with adhoc query, integration with spreadsheets, proactive alerting, Scorecards and so on. • Should provide capabilities to create KPIs to measure progress and performance over time and graphically communicate strategy & strategic dynamics using Strategy maps, Cause and Effect diagrams, and Custom views. Intuitive and dense visualizations should be available.	
ICCC/FR/51.04		Application should enable the operators to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system should carry the following tasks: • Connect to a variety of data sources • Analyze the result set	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Visualize the results • Predict outcomes • Prescribe options for DSS (Decision Support System)	
ICCC/FR/51.05		Analytics Engine should provide visualizations dashboard and ensure following features: • It should allow changing visual attributes of a graph in the visualization workspace / dashboard. • User should not be allowed to alter the graph/visualization definition.	
ICCC/FR/51.06		• The platform should display the threat level based on the frequency of a particular type of alert and criticality of the alerts using Colour coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts.	
ICCC/FR/52.01	Data Aggregation, Normalization and Access	• The Common integrated smart city platform shall be able to normalize the data coming from different devices of various OEMs. It shall support integration with multiple vendors - The City will be using various device vendors for various urban services. For example, various vendors of smart elements will be used for deployment and each will be generating data in their own format. Hence, Smart City platform should be able to define its own data model for each urban service like parking, waste, lighting, transport etc. and map data from different device vendors to the common data model • This data should be exposed to application eco system using secure APIs using API keys • The attributes of the API key(s) should restrict / allow access to relevant data, i.e. (the attributes can be like: specific domain (either parking or lighting or waste etc., or combination of these), RO / RW /, specific to tenant (city, street within city etc.)). • Multitenant City operations Dashboard: City software platform Dashboard should display only relevant data (associated geographical data) for the user who logs in. • The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Agnostics to sensor technologies such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera • The platform should allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration. • The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers. • The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• ICCC platform comprising of Pre-Integrated Visualization layer & IOT platform proposed should be deployed in at least 1 city in India operational for more than a year with 5 use cases mentioned in the tender.	
ICCC/FR/52.02	GIS Map Support	• System should support GIS maps like ESRI, map box, Open Street, open GIS etc..,	
ICCC/FR/52.03	Location engine	• Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities • Geospatial calculation: calculates distance between two, or more, locations on the map • Location-based tracking: locates and traces devices on the map • All maps shall have to be dynamic and be able to display on a standard mobile device (android, windows, IOS)	
ICCC/FR/52.04	Service Catalog management	• The Service catalogue management module should allow to categorize the externalized and non-externalized services into logical groups by creating the service catalogues. In addition, system should allow manage the service catalogues by adding, modifying, or deleting the catalogue details • The service catalogue and criticality of the services shall have to be definable by respective user organization and • System shall provide catalogue wise number of services / requests serviced during any period of query along with a location map of origin of various service requests to be able to analyse / co-relate to ground situations of those geographic regions	
ICCC/FR/52.05	Developer Program tools	• Platform OEM should provide online Developer Program tools that help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. OEM should have technology labs via an online public facing web interface. These labs should be available 24x7	
ICCC/FR/52.06	Authentication, Authorization	• System should support standard Authentication, Authorization Methods	
ICCC/FR/52.07	API Repository / API Guide	• Normalized APIs for the City Application domains should be available (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality. • Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future) • OEM of the platform should submit their data sheet, ordering guide & API document available on the public domain.	
ICCC/FR/52.08	Platform Upgrades and maintenance	• The OEM should be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/52.09	Platform hosting	• Platform should support both cloud hosted and On-premise solution and shall be provided with On-premise solution for Common Integrated Data Center	
ICCC/FR/52.10	Platform functionality	• API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs • User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions • Application management: Provides role-based access view to applications on dashboard • Enabling analytics: Time shifted and real-time data available for big data and analytics • The platform should also be able to bring in other e-governance data as i-frames in the command and control center dashboard • All of these data should be rendered / visualized on the command and control center dashboard.	
ICCC/FR/52.11	ICCC Operations	• The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable. • The solution should have the capability to integrate with GIS • The solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources. • The solution should provide operators and managers with a management dashboard that provides a real-time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be color coded. • The solution shall provide the “day to day operation”, “Common Operating Picture” and situational awareness to the center and participating agencies during these modes of operation • It shall provide complete view of sensors, facilities, e-governance, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine • It shall provide a uniform, coherent, user-friendly and standardized interface • It shall provide possibility to connect to workstations and accessible via web browser • The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard • The solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes • It shall be possible to combine the different views onto a single screen or a multi-monitor workstation • The solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The solution should provide ability to extract data in desired formats for publishing and interfacing purposes • The solution should provide ability to attach documents and other artifacts to incidents and other entities • The solution is required to issue, log, track, manage and report on all activities underway during these modes of operation: • recovery • incident simulation	
ICCC/FR/52.12	Integration capabilities	• The Platform shall also be able to integrate, connect, and correlate information from CCTV, IoT Platform and other IT & non-IT systems, providing rule based information drawn from various sub-systems for an alert. • Platform should support on the fly deployment of Sensors. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown. • Platform should support the development of Integrations for legacy SCADA systems such as OPC UA and/or serial communication, messaging protocols such as MQTT, Stomp, AMQP etc. This is in order to seamlessly integrate the existing legacy systems and new systems coming in to the Smart City. The integration to the external legacy sub-systems current or futuristic should be on real-time basis and not on offline basis.	
ICCC/FR/52.13	Edge Computing	• Platform Should support integrating standard edge appliance used to: - connect industrial protocol devices, - provide secure connection to cloud infrastructure, - provide remote lifecycle management including software/firmware downloads and upgrades, - Provide remote management, self-registration, and local administrative interface. • Should support edge appliance integration to abstract downstream industrial protocols and upstream internet protocols. • Edge appliance should be supported in three form factors : - Over the Pole, - in street Cabinet - street appliances - or in ICCC in an appropriate rack-multiplexed feeds management • Should be light weight. • Smart City platform should be functionally complete on the edge, providing local processing of events, contextualization, transformation, analytics, decisions and controls. Business relevant events only passed to DC. • Smart City platform should allow to set or change the behavior on the edge through policies, which could be defined through Data Center Integrated Platform.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Edge devices should learn the behavior as analyzing the data to create better decisions with time. Share the outcomes with the cloud/platform to impact other edges. • Should support management tools to view, analyze, report on and modify the edge configurations. • Edges and cloud/On premise instances of platform should create a logical cluster to distribute the workload dynamically between the nodes, if and when applicable. • Edge software should not be dependent on sensors and devices or protocols. Same software blueprint should be deployed and running on all edges without losing the performance or objective of the required edge analytics. The system shall be able to accommodate different edge analytical software as per the devices being integrated and each of these shall be usable on same deployed servers or other shared servers as per need. Data and Configurations can be different from edge to edge.	
ICCC/FR/52.14	Resiliency	• Should provide ways to define policies that make applications or things respond to external environments • The Smart City platform should support integration to collaboration tools to bring multiple stake holders and responders to respond an emergency or an urban services event. • The Smart city platform should be able to alert any incidents in the network proactively on command and control center • The smart city platform should have integrations with the network layer to proactively monitor any incidents on the network for active troubleshooting and triaging	
ICCC/FR/52.15	API Based Open Platform	• Should provide urban services' API(s) to develop operation applications for each of the Urban Services domains. For example, the lighting operator of the City should be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application should also have the ability to access data from other domains like environment based on the access control configured in the system. • The smart city platform should have API Management capabilities like API Security, API Metering, API Monetization • The smart city platform ~~is~~ should be able to provide API access based on roles and access control policies defined for each user and the key issued to that user • The vendor should have already documented different Urban Services APIs using which applications can be developed • The vendor should be able to demonstrate existing applications that are developed using these urban services APIs • Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc.…) • Enables City and/or its partners to write software adaptors based on the API(s) provided by device	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		vendors and have the ability to control, monitor and collect the data from these street devices	
ICCC/FR/52.16	Trending Service	• System should provide trends in graphical representation from data sources over a period of time. Trends should allow to monitor and analyze device performance over time.	
ICCC/FR/52.17	Policies and Events	• System should allow policy creation to set of rules that control the behavior of infrastructure items. Each policy should a set of conditions that activate the behavior it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs. However, all manual overrides and actions / sequences carried out post an event shall all be traceable to every user and in time sequence as well, so as to be able to improvise on any future similar occurrences • System should provision to defines a set of conditions that can be used to trigger an event-based policy	
ICCC/FR/52.18	Video Integration	• Platform should be capable of integrating the existing & new surveillance camera and provide viewing of camera feeds on visualization dashboard or display server • Platform shall have video module to Integrate any vendor video surveillance management solution • Display module should have capability to control multiscreen display wall in sync with operator console • Video module of Platform should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location • Video module should post data to Integrated platform on a regular basis for Camera details, notification and status • If the remote station is viewing in low resolution (non-HD), the stream to remote viewing location should not be using HD bandwidth, but dynamically should change to lower bandwidth • If the remote viewing station is viewing this camera in full screen 1080P, then it should dynamically increase the bandwidth to provide HD experience • City Operation & Control platform should use dynamic channel coverage for video stream function for efficient bandwidth usage and only transmits video stream required to display on monitor to maximize bandwidth efficiency • Platform shall process and transmit video streams adaptive to each video request from a display server to optimize network bandwidth usage • Regardless of the numbers or the types of video input, platform shall be able to batch process and transmit 15 Full HD / 36HD video streams at all times • Platform shall be able to distribute real-time video streams to both display server and main operating server without any loss in original video quality	
ICCC/FR/52.19	Export Formats	Should support export of the analysis into following formats: • XML/JSON	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Excel • PDF • CSV	
ICCC/FR/52.20	Infrastructure Operations	• The OS instances should be hardened as per the latest CIS-CAT benchmarks with target of T-3 DC compliance requirement or >85% compliance. All actions should be audit-logged. Hardened OS shall have only required applications, process and permissions. All components should be hardened as per industry standards	
ICCC/FR/52.21	API & Interface Security	• The access to data should be highly secure and efficient. • Access to the platform API(s) should be secured using API keys. • Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains. • Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where ICCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.	
ICCC/FR/52.22	Infrastructure Security	• Platform should support user encrypted storage volumes. Restrict inbound access from public network only on secure ports via DMZ proxy instances. SSH access is restricted with secure key pair and from designated jump hosts alone. User management and authentication is tied to RSCL defined SSO for each access to the databases and physical hardware systems or for configuration systems. Daily reports on system level accesses, system usage performance reports shall be enabled on a dynamic dashboard and any breach in access detected at a later date shall lead to due penalties applicable to the MSI and to the unauthorized user under the IT Act of the Government of India or the state notifications from time to time • System should support following security features - User encrypted storage volumes. - Restrict inbound access from public network only on secure ports via DMZ proxy instances - SSH access is restricted with secure key pair and from designated jump hosts alone. - User management and authentication is tied to Corporate SSO. - Platform should have appropriate technical controls in place to prevent attacks that target virtual infrastructure • Platform should have appropriate controls in place to detect source code security defects, functionalities for any outsourced software development activities from suppliers, open source libraries	
ICCC/FR/52.23	Data Security & Integrity	• Data Governance / RBAC: Platform should support data governance & stewardship model, in which roles, responsibilities are clearly defined, assigned, implemented, documented and communicated	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Data Protection / Production Data integrity: Platform should support procedure in place to ensure production data shall not be replicated or used in non-production environment • Data Protection / Data at rest: Platform should support encryption for tenant data at rest (on disk/storage) • Data Retention: Platform should support capabilities to enforce tenant data retention policies • Data recover & restore: Platform should support capability to recover and restore data in case of a failure or data loss. • Data disclosure & privacy: Platform should disclose data attributes, elements collected from source. All the attributes should be disclosed & appraised to data owner. With appropriate approval from City authority, Platform should have ability to encrypt sensitive data element at rest.	
ICCC/FR/52.24	Release Operations	• Critical production assets: Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses and these could be traceable online as well • Patch Management: Platform should have capabilities to patch vulnerabilities across VM infrastructure, applications and systems • Patch timeline / notifications: Platform vendor should provide risk-based systems patching time frames to tenants based on request • Secure SDLC: Platform should support automated source code analysis tool to detect security anomalies / defects in code prior to production	
ICCC/FR/52.25	Scaling, Capacity Provisioning parameters	• Platform should be scalable and should support capacity provisioning additional CPU, RAM to existing VM, Cloud infrastructure • Platform should have tools to monitors the healthiness of the individual tenants and status of CPU, Memory performance • The platform shall send alerts to the user once it exceeds certain limits in terms of CPU and Memory performance	
ICCC/FR/52.26	Business Operations	• Audit & logging: Platform should support centralized logging & auditing framework. Physical and logical user access to audit logs restricted to authorized personnel only. • Legal / Supplier chain agreements: Platform provider vendor should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs) between providers and customers • Critical production assets: Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/52.27	Support Field Responder Mobile Apps	• Should support integrated Mobile Application for Android, Windows and iOS for capturing real-time information from the field response team using Mobile-Standard Operating Procedure.	
ICCC/FR/52.28	High Availability	• Platform shall have no single point of failure. • Software & hardware fault shall not result total system failure • All failure should report relevant error messages to the user • Platform vendor shall provide supporting infrastructure, appropriate tools to measure & monitor system availability and automated notification for system failure and unavailability	
ICCC/FR/52.29	Logging	• Platform should support logging frame with following functionalities - Logs shall readable in ASCII plaintext or UTF-8 format - All logs shall be timestamped - Log events shall capture user activities, applications, system & network IDPS messages - Centralized & secure log repositories to all log events - System logging shall be provided for all successful and unsuccessful login attempts and for all super user activities - Platform should implement mechanisms to trigger alerts and facilitate users to analyze and review logs efficiently - All critical logs are secured and sent to archive - Centralized logging shall be configurable to report for exceptions and generate reports based on desired filters • Appropriate controls shall be put in place to ensure outage of the central log repository does not result in any loss of logs • The central syslog shall be able to normalize logs from wide variety of platforms / components to Common Event Format (CEF) to ease of use for monitoring and analysis and support logical data segregation so that the different user groups can only view their own managed equipment logs • Central syslog system shall have sufficient disk storage to keep the logs for 1 year to facilitate incident response investigation • Logging should have following retrieval time - Timeline : Log Duration 6 Hrs. : 0 – 30 days 1 day : 30 – 90 days 5 days : Older than 90 days	
ICCC/FR/52.30	Performance Monitoring	Performance monitoring tool shall include following functionalities • Identify infra and/or application components between the user and backend servers that is causing the problems • Providing key performance indicators	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Identify the inter-dependencies between application & infra components • Able to provide network/ system node causing the problem • Provide email, SMS and/or mobile alert mechanism if performances fall below predefined thresholds • Performance monitoring shall not adversely affect the performance of the platform • Should display the threat level based on the number of alerts and criticality of the alerts using Color coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts.	
ICCC/FR/52.31	Database monitoring	• Platform should support database monitoring tool for DB health checks to monitor - Memory allocation, usage and contention - Disk I/O usage - CPU usage for a particular transition - Number of buffers, buffer size and usage - Active locks and locks contention, including waiting time • List of users (complete or selected) with their access rights	
ICCC/FR/52.32	Platform Environment	• Platform provider shall have 3 environments - Development environment - QA environment - Production environment • All 3 environments shall be physically / logically separated • All should have same system & application software versions	
ICCC/FR/52.33	Platform Software	• Platform provider shall provide complete information on all platform software deployed indicating clearly the software versions, quantity of licenses, functions, type of license (one time or annual recurring) • Platform provider shall transfer all licenses with maintenance service supports to authority • There shall be no use of untested freeware or shareware and proprietary software that is not approved by RSCL	
ICCC/FR/52.34	Backup and Recovery	• Platform backup and recovery solution functionality shall support following requirements - Perform online database backup and recovery - Support full, incremental, scheduled and on-demand backups - Perform backup verification to ensure integrity of backup - Perform automatic drive cleaning using pre-mounted cleaning tape • Provide comprehensive reporting and analysis functions	
ICCC/FR/52.35	Alarm Management Module	• The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		module shall provide a real- time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting • The alarm management module shall provide interface and navigational tools through the client including;	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
Key Integration Requirement			
ICCC/FR/53.01	Integration with SWM for mentioned activities	Real-time tracking of containers and solid waste collection vehicles with automated warning system for deviations from routes assigned.	
ICCC/FR/53.02		Grievance Redressal system to receive complaints online or by telephone, facsimile, email or in person and initiate action for dispatching waste management service request calls to the appropriate internal and field personnel and tracking progress of waste management service requests against pre-determined KPIs	
ICCC/FR/53.03		Maintain asset information of all vehicles, containers, depots, bins, etc.	
ICCC/FR/53.04		Waste Management Module of SWM for real time tracking of requests, its assignment to concerned officials, subsequent actions taken up to its closure	
ICCC/FR/53.05		Attendance module of SWM to enable real time monitoring of attendance for the field staff and subsequently its integration with Payroll	
ICCC/FR/53.06		Billing and Collection module of SWM for billing and payments associated with the waste collection agency/residents, as applicable, using the ERP system.	
ICCC/FR/53.07		Daily, weekly, monthly reports on item-wise, dept. wise and activity wise details	
ICCC/FR/53.08		Attendance reports	
ICCC/FR/53.09		Grievance reports showcasing in-progress, resolved and unattended complaints	
ICCC/FR/53.10		Consolidated report generation on garbage depots activity	
ICCC/FR/53.11		Monitoring the activity and payment to contractors/ workers etc.	
ICCC/FR/53.12		Billing and collection reports, etc.	
ICCC/FR/53.13	Integration with ATCS, TVDS, PAS and VaMS	Recognize, identify and monitor the infracting vehicles in real-time / off-line mode for various violations at junctions and in streets.	
ICCC/FR/53.14		The system shall have the ANPR Non-intrusive modes of enforcement on TVDS and Speed.	
ICCC/FR/53.15		The system at the ICCC shall be integrated with the E-Challan system to enable E-Challan generation, payment and billing process.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/53.16		Public Address (PA) System to disseminate the information to the citizen particularly emergency situation messages to reach quickly.	
ICCC/FR/53.17		The system shall be able to integrate other network PA systems or third party application systems where the alerts are generated to broadcast messages at ICCC.	
ICCC/FR/53.18		The system shall be able to generate various statistics, reports & MIS from time to time at ICCC.	
ICCC/FR/53.19		Variable Message Signboards (VaMS) shall provide feedback to the ICCC on the VaMS status of Active / Inactive.	
ICCC/FR/53.20		The system shall maintain the history of messages archived for future reference and analysis.	
ICCC/FR/53.21		The ATCS system shall provide multiple interfaces to share the data seamlessly to different sub systems e.g. signalling system to configure and determine the traffic signal duration based on the traffic congestion, weather conditions, traffic pattern and other factors.	
ICCC/FR/53.22		The system at the ICCC shall feed the traffic density information to the associated junctions of critical junction subsystem to determine the expected traffic from its previous junction and traffic signal duration.	
ICCC/FR/53.23		The system at the ICCC shall integrate with the Adaptive traffic control System module to support TVDS and Transit Signal Priority.	
ICCC/FR/53.24	Integration with e-Governance Solutions	ICCC shall also monitor the different MIS reports generated from various systems like online citizen services portal and report to RSCL officials so that corrective actions can be taken to increase the usage of online systems by the citizens of Rourkela.	
ICCC/FR/53.25		Automatically detect when citizen services are needed as indicated but not limited to the following: • Monitor and control from a single point the water quantity, quality, treatment and distribution process in real time. • Real time streaming analytics on tweets and social media events, blogs, grievances and discussion portal with data quality and content categorization. Dynamically sense the citizen environment and mitigate government service disruptions through social media and other citizen data	
ICCC/FR/53.26		The system must provide Incident Management Services to facilitate the management of emergency response and recovery operations like fire, police, ambulances, theft, violence, etc.	
ICCC/FR/53.27		Shall support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.	
ICCC/FR/53.28		Shall support for sudden critical events and linkage to standard operating procedures automatically without human intervention.	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/53.29		Shall support for multiple incidents with both segregated and/or overlapping management and response teams.	
ICCC/FR/53.30		Shall support Geospatial rendering of event and incident information.	
ICCC/FR/53.31		Shall support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.	
ICCC/FR/53.32		Shall support incorporation of resource database for mobilizing the resources for response. Contact details of all the concerned department officials to be maintained in the database and automated SMS and e-mail alerts to be sent whenever required.	
ICCC/FR/53.33		Shall provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents shall be captured in standard formats to facilitate incident correlation and reporting.	
ICCC/FR/53.34		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems	
ICCC/FR/53.35		Shall provide detailed reports and summary views to multiple users based on their roles.	
ICCC/FR/53.36		A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.	
ICCC/FR/53.37		Provide User-defined forms as well as Standard Incident Command Forms for incident management	
ICCC/FR/53.38		Energy and Water Optimization shall be present where algorithms shall optimize energy and water use with input from weather forecast, electricity pricing, future energy demands, electricity consumption, water reservoir levels, etc. and leverage integration from SCADA based network.	
ICCC/FR/53.39		ICCC shall have the capability to take environmental condition feed from meteorological department or Air Quality Monitoring System or any other applicable inputs. In case of rain predictions, ICCC shall automatically alert departments for preventive maintenance of water logging issues.	
ICCC/FR/53.40	Integration with Safety & Surveillance	ICCC Will be required to integrate with Safety and Surveillance solution using Open API standards.	
ICCC/FR/53.41		ICCC will be required to receive the feeds from Safety and Surveillance solution related events.	
ICCC/FR/53.42		ICCC will be required to receive the Public safety related videos in real time from Safety and Surveillance solution for the selected locations	
ICCC/FR/53.43		All the information received from Safety and Surveillance solution will be mapped on GIS map	
ICCC/FR/53.44		All the information received from Safety and Surveillance will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard	
ICCC/FR/53.45		ICCC should also be able to trigger the commands/Alerts (If required) to Safety and Surveillance sub system	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
ICCC/FR/53.46		The video feeds received will be saved in DC	
ICCC/FR/53.47	Integration with Environmental Sensor	ICCC will be required to integrate with Environmental Management sub System using Open API standards	
ICCC/FR/53.48		ICCC should be able to map this information on the GIS layer and help authority monitor the environment condition across the city.	
ICCC/FR/53.49		ICCC should also be able to trigger the commands / alerts (if required) to the respective sub system.	
ICCC/FR/53.50		All the information received from Environmental management sub system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard.	
ICCC/FR/53.51	Integration with City Wi-Fi	ICCC will be required to integrate with Wi-Fi Hotspots sub System using Open API standards to receive the feeds related to • Wi-Fi status across city • KPI's related to free Wi-Fi	
ICCC/FR/53.52		ICCC should be able to map this information on the GIS layer and help the authority monitor the Wi-Fi Hotspots across the city.	
ICCC/FR/53.53		ICCC should also be able to trigger the commands / alerts (if required) to the respective sub system	
ICCC/FR/53.54		All the information received from Wi-Fi Hotspots sub system will get into Analytics layer of ICCC and provide useful insights and KPI's over dashboard	
ICCC/FR/54.01	Building Management System (BMS)	BMS shall be installed at ICCC building to provide the following functionalities as a minimum but not limited to: • Monitoring and control of building automation (cooling/heating control, ventilation control) • Monitoring and control of internal and external lighting in the building • Monitoring of electrical power distribution system through multi-function meters • Monitoring of DG Parameters (as applicable) • Integration with the Fire detection and alarm system • Monitor and manage energy consumption throughout the building for the purpose of tracking quality and usage of electricity • Integration with video surveillance system inside ICCC • Integration with access control • Monitoring and control of UPS.	
ICCC/FR/54.02		Integration with HVAC System: • Monitor and control ON/Off status and generate alarms. • Monitor and control temperature, pressure, humidity being maintained by the AC. • Monitor energy consumption related to HVAC; • BMS shall integrate with following HVAC components at a minimum (as applicable) for comprehensive	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		monitoring and control: - Central Chiller Water Systems; - Air Handling Units (AHU); - Fan Coil Units (FCU); - Treated Fresh Air (TFA) Fans; - Ventilation and Exhaust Fans; - Pressurization Fans.	
ICCC/FR/54.03		Integration with Lighting System: • Functionality: - Lighting control through time based sensors • Control Required: - MCCB On/Off command for internal and external lighting - Scheduling of On/Off of lights through BMS software • Monitoring Required: - MCCB and On/Off status	
ICCC/FR/54.04		Integration with Electrical Power Distribution System: • Monitoring and Control functions for electrical power distribution system is as follows: - Maximum demand monitoring - Break status monitoring - Trip status monitoring - On/Off status • Breaker On/Off, trip Monitoring on a real-time basis • Status to be monitored (ON/OFF/Trip Status and relay indications and alarm): - HT and LT Boards - ON/OFF station at all other panels - Transformers to be monitored - Trip status	
ICCC/FR/54.05		Integration with DG Parameters (as applicable): • DG Sets to be monitored • Monitoring of following parameters to be done: - DG On/Off status - Frequency - Trip status - Engine fail to start (U/V Trip) - Alternator field failure - Alternator fail to built-up voltage - DG Trip due to earth fault - DG Trip due to overload - DG Room Temperature - Inlet Cooling Water Temperature - Outlet Cooling Water Temperature - Cooling water flow OK - Day tank low/high - HSD Tank low/high - DG over speed feedback - Low lube oil pressure - Common engine fault alarm - Auto synchronizing panel breaker status - Battery weak	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		- Battery low voltage alarm - PLC controller failure alarm - Emergency stop operated - Reversed power - Oil pressure - Common shutdown • Control: - Auto sync panel breaker On/Off control - Emergency stop • Field Devices: - Day tank and HSD tank fuel level measurement using tank level sensors - Day tank and HSD tank flow measurement using flow switch sensors Fuel tank temperature monitoring	
ICCC/FR/54.06		Integration with Fire Alarm and Detection System: IP based Fire alarm system shall integrate with the BMS and the status of the fire detection system shall appear on BMS.	
ICCC/FR/54.07		Integration with UPS: UPS shall be integrated with BMS via open protocols. Monitoring of following parameters shall be done via BMS: • Battery voltage • DC voltage • Battery charging/discharging status • Estimated time before shutdown during battery discharge • Rectifier failure alarm • Battery discharge status Low battery warning alarm	
ICCC/FR/54.08		Integration with Energy Monitoring System: • The energy monitoring software shall be a web-enabled monitoring system intended to monitor the entire electrical distribution infrastructure, from incoming utility feeds to low voltage distribution points. • The system shall be designed to monitor and manage energy consumption throughout the facility, whether within a single building or across a network of buildings, to improve energy availability and reliability, and to measure and manage energy efficiency. • Software required for energy monitoring shall be an integral part of BMS and shall provide a seamless user experience for managing all systems integrated with the BMS. • Key features shall include: - Data acquisition for metering devices, sensors and other intelligent electric devices. - Graphical, real time displays of electrical distribution system for monitoring of voltage, current, power, frequency, THD, power factor, individual harmonics etc. - Reporting tools with standard report templates which shall include billing reports, energy usage reports, trend reports, energy comparison reports,	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		alarms and exception reports etc. - Power Quality Analysis - Energy Analytics and Measurement - Energy Budgeting - Energy predictive analysis - Interactive historical data display and trending - Demand Limiting / Load Rolling - Real Time Data Tables with Standard Views - Interactive Alarm Analysis with Standard Views - Power Factor monitoring and reporting - Interoperability with disparate devices and systems; and Third Party Device Integration through Modbus RTU and Modbus TCP protocols	
ICCC/FR/54.09		Integration with Video Surveillance System: • For a comprehensive BMS and to provide a uniform view of all systems, video surveillance with a fully IP based Network Video Recording (NVR) system shall be integrated with the BMS. This shall work in conjunction with access control and intrusion detection system to provide one-stop security solution. • BMS shall start recording video stream upon triggering from intruder alarm system and access control system. • The integrated system shall be used through the video surveillance system's own User Interface Client and also through the integrated user interface of the BMS system. • Following functionalities shall be supported by BMS upon integration with video surveillance system: - Web usage and client application both shall be supported; - The BMS shall support receiving of real time values, trends, alarms and event logs from the connected systems. Different levels of logs (e.g. warning, error, info) shall be available. - The BMS shall support modification of set points, time schedules and manual (override) controls in the connected systems. - BMS shall support an event mapping mechanism for triggering of functions, e.g. starting video recording and turning on lights from events like unauthorised access attempt. - BMS shall include centralized alarm dispatching features for all connected systems, using e.g. SMS and email. The system shall support triggering of functions based on the events from the other connected systems. The BMS shall be modular in structure, consisting of services, which are flexible to add, configure and to update.	
ICCC/FR/54.10		Integration with Access Control System: • The Access Control shall be intended to control physical access to premises and detects unauthorized	

S. No.	Description		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		access. The Access Control shall ideally be implemented as one unified system with smart network controllers and interface panels. • Access control system has the capability to classify users so that they can have access only to spaces where they are allowed to enter according to programmed time schedules. • Access Control shall be integrated with the BMS in order to provide a unified solution for security management. • Following functionalities shall be supported by BMS upon integration with access control: - Access control and intrusion system shall be monitored through a graphical user interface. Web usage and client application both shall be supported. - The BMS shall support receiving of real time values, trends, alarms and event logs from the connected systems. Different levels of logs (e.g. warning, error, info) shall be available. - The BMS shall support modification of set points, time schedules and manual (override) controls in the connected systems. The BMS shall be modular in structure, consisting of services, which are flexible to add, configure and to update.	
ICCC/FR/54.11		Integration with DG Synchronization, Auto Load Control and Auto Mains Failure Panel: Integration shall be with DG Synchronization, auto load control and auto mains failure panel to give status to BMS.	

IOT and SOA Framework

IOT Framework

- The Platform should support the connectivity with multiple protocols like AMQP, XMPP, CoAP, MQTT, XML/JSON etc.
- It should be modular to be able to write new adaptors for devices not following any standard protocol.
- Should support mediate data into a common format and put on a big data platform or equivalent.
- Should be able to perform Device Management and perform OTA firmware updates.
- Should be able to perform billing and usage reports.
- Should be on premise, private cloud based scalable solution.
- Should have a visualization layer and reporting layer with integration capability
- Should have an API based interface to expose data.
- Should support in accelerate the development of IoT solutions development from idea, to prototype, to production having pre-build libraries and attributes
- IoT platform should offer pre build APIs, tools and templates for customers.
- APIs, tools and templates could be built for same vertical applications like automotive, building, healthcare, metering, etc.

- Pre build tools and SDK for building mobile apps on different OS like Android, Windows, iOS to deploy IoT mobile applications in future.
- Network Access and Standards:
  - LoRA network support with Lora WAN, LoRA Network server with min 853 to 868 MHz or better
  - 3GPP specs defined support for Narrow Band – IOT.
  - Wi-Fi over 802.11 support as standard protocol
  - IPv4/IPv6 Support for all kinds of access network.
  - 2G/3G/4G/5G or better eUICC SIM network support.
  - Global Connectivity platform support for multi-operator SIM cards profile for GSM based devices.
- Should be able to support Cloud and infrastructure support
- Should support discovery of meaning patterns in data collected from devices/sensors/instruments in conjunction with other application-specific externally imported data. This component provides a creation, execution, and visualization environment for all types of analytics including batch and real-time—based on Complex Event Processing— for creating data insights that can be used for business analysis and/or monetized by sharing insights with partners.
- IoT Data Analytics should covers various types of analytical modelling such as descriptive, predictive, prescriptive—KPIs, social media, and geo-fencing, predictive/propensity determination, and prescriptive/ recommendations.
- The Business and operation support system should provide a consolidated end-to-end view of devices, gateways, and network information. This module helps IoT operators automate and prioritize key operational tasks, reduce downtime through faster resolution of infrastructure issues, improve service quality, and optimize human and financial resources needed for daily operations. The as above module drives operational efficiency and service reliability in multiple ways:
- Should be able to identify problems quickly through automated problem correlation and root- cause analysis across multiple infrastructure domains, and determines impact on services
- Should be able to automate major steps in the problem-resolution process, reducing service outage time
- Should have console GUI, the IOT Console should supports business critical service operations and processes. It provides real time data and metrics-allowing reacting to business change as it happens, detecting service failures and protecting vital revenue streams.

SOA Framework

- A single unified platform and anytime service registry to be built to govern both services and APIs such as REST, SOAP and legacy systems – Thus managing internal and external service assets, whether they reside on-premises or in the cloud
- Facilitate integration of the solution with existing systems of Rourkela Municipal Enterprise Systems and To be Proposed System too.
- Develop provisions for a scalable system which can integrate with more devices of the same kind (as those deployed today) and can integrate with future applications and sensors through open standards and data exchange mechanisms
- Prevent duplication by managing services and endpoints in the Service Repository
- The SOA Policy Manager making it easy to create and apply policies to ensure security, quality, and compliance
- Development of web-services for Integration with other systems
- Development and Enablement of Web Services for integration with external systems and access by external systems
- Support the IoT applications integration of Smart city Application on to the IoT Platform

and seamless integration of the smart cities applications

- Following SOA Design Principles should be the Part of ICCC Platform while it integrates with City Street Infra Layer and other enterprise Systems. They are:
  - Standardized service contract – Implementing a Standardized Contract
  - Service loose coupling – Minimize Dependencies
  - Service abstraction – Minimize the Availability of Meta Information
  - Service reusability – Generic and Reusable Logic and contract
  - Service autonomy – Independent functional Boundary and runtime environment
  - Service statelessness – Adaptive and State Management Free Logic
  - Service discoverability
  - Service composability – maximize Composability

Minimum Technical Requirements

Technical Requirements for ICCC: IT Components

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
1. General			
ICCC/TR/1.01	Space Requirements	Approximate space of around 20000 sq.ft is proposed for the development of the Integrated Command and Control Center. The proposed layout comprises of ICCC building with G+3 floor construction. Following components are proposed to be part of the ICCC building: - Video Hall - Situation Room - Teleconference Room - Meeting Room - Cabins - Training Room - HelpDesk - Board Room - Data Centre - Waiting Area - Any other area as appropriate	
2. Video Display Wall			
ICCC/TR/2.01	Technology	HD IPS LED Display, Direct LED Backlight	
ICCC/TR/2.02	Display Unit	The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should have LED as its light source with ultra-thin configuration.	
ICCC/TR/2.03	Screen Size	Each cube size to be 70” (70 Inches diagonally) or more with complete configuration of (8 cubes x 2 cubes) with covered base. All cubes have to be of the exactly same size, configuration and model wise mandatorily. The wall to be installed in curved fashion with all required support system like Controller / stand for DLP Cubes / Interfaces / Connecting cables.	
ICCC/TR/2.04	Resolution	The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should have LED as its light source with ultra-thin configuration.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/2.05	Aspect Ratio	16:9	
ICCC/TR/2.06	Brightness	The brightness uniformity of the VDM shall be >95%.	
ICCC/TR/2.07	Contrast Ratio	Dynamic contrast should be 1,200,000:1 or better	
ICCC/TR/2.08	Wall Uptime	The light source lifetime of the LED shall be at least 90,000 hours. This should be certified by the OEM.	
ICCC/TR/2.09	Viewing Angle	VDW shall provide minimum viewing angles of: • Horizontal - ½ gain: ±35 degrees, 1/10 gain: ±57degrees • Vertical - ½ gain ±10 degrees, 1/10 gain: ±28 degrees	
ICCC/TR/2.10	Screen to Screen gap	The inter screen gap (bezel gap) should be <0.4 mm.	
ICCC/TR/2.11	Input	Analog D-sub/Ethernet/Digital DVI/Digital HDMI (as per solution)	
ICCC/TR/2.12	Operating Temperature	As per City requirement	
ICCC/TR/2.13	Relative Humidity conditions for operation	The VDW shall have a relative humidity of 20% to 80%, non-condensing or better.	
ICCC/TR/2.14	Power	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz. Power consumption of each cube shall be less than 350W.	
ICCC/TR/2.15	Warranty	5 Years	
ICCC/TR/2.16	Others	• The Cube shall have redundancy in power supply, LED light source. • Each cube of the VDW shall have its own IP address and on-board web server to provide standard information like status and health. • RS232 control (with loop-through) • On Screen Display (OSD) • IR remote control • Flicker free image on the Large Screen • The dashboard shall be capable of simultaneously displaying one (1) to one hundred (100) independent sets of information on the video display wall. Specific outputs to be displayed shall be chosen by operators. • VDW shall be capable of displaying high definition (HD) and standard definition (SD) content. • Auto colour and brightness management mechanism to be provided. • Screen should have an anti-reflective glass backing to prevent bulging. • All video display cubes shall have a consistent image quality and uniform brightness across the display wall. • Each display cube shall not exceed a thermal dissipation of eight hundred (800) BTU per hour under normal operating conditions.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• A pedestal shall be provided to support the VDW. Pedestal shall be physically secured to the concrete floor of the building. Support structure shall be with a laminate finish. Support structure shall incorporate sound proofing to prevent noise penetration from the equipment into the command centre.	
3. Video Wall Controller			
ICCC/TR/3.01	Controller	Controller to control Video wall in a matrix as per requirement along with software	
ICCC/TR/3.02	Chassis	19" Rack mount	
ICCC/TR/3.03	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better	
ICCC/TR/3.04	Operating System	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc	
ICCC/TR/3.05	RAM	16 GB DDR3 ECC RAM	
ICCC/TR/3.06	HDD	2x500 GB 7200 RPM HDD (Configured in RAID 0)	
ICCC/TR/3.07	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports	
ICCC/TR/3.08	RAID	RAID 0, 1, 5, 10 or more support	
ICCC/TR/3.09	Power Supply	(1+1) Redundant hot swappable	
ICCC/TR/3.10	Input/Output Support	DVI/HDMI/USB/ LAN/ VGA/SATA port	
ICCC/TR/3.11	Accessories	104 key Keyboard and Optical USB mouse	
ICCC/TR/3.12	USB Ports	Minimum 4 USB Ports	
ICCC/TR/3.13	Redundancy Support	Power Supply, HDD, LAN port & Controller	
ICCC/TR/3.14	Scalability	Display multiple source windows in any size, anywhere on the wall	
ICCC/TR/3.15	Control functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate	
ICCC/TR/3.16	Inputs	To connect to minimum 2 sources through HDMI	
ICCC/TR/3.17	Output	To connect to minimum 16 Displays through HDMI	
ICCC/TR/3.18	Operating Temperature	As per City requirement	
ICCC/TR/3.19	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units	
4. Video Wall Management Software			
ICCC/TR/4.01	Display & Scaling	Display multiple sources anywhere on display up to any size	
ICCC/TR/4.02	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows	
ICCC/TR/4.03	Scenarios management	Save and load desktop layouts from local or remote machines	
ICCC/TR/4.04	Layout Management	Support all layout from input sources, Internet Explorer, desktop and remote desktop application	
ICCC/TR/4.05	Multi View Option	Multiple view of portions or regions of Desktop, multiple application can view from single desktop Ability to display multiple sources anywhere on video display wall (VDW) in any size Ability to stretch, re-position, and resize any video source on any display device	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		Ability to treat the VDW as a single display. It shall act as a single canvas with no pixel separation	
ICCC/TR/4.06	Other Features	SMTP support	
ICCC/TR/4.07		Remote Control over LAN	
ICCC/TR/4.08		Alarm management	
ICCC/TR/4.09		Remote management	
ICCC/TR/4.10		Multiple concurrent client	
ICCC/TR/4.11		KVM support	
ICCC/TR/4.12	Cube Management	Cube Health Monitoring	
ICCC/TR/4.13		Pop-Up Alert Service	
ICCC/TR/4.14		Graphical User Interface	
ICCC/TR/4.15		Setting all projection modules to a common brightness target, which can be either static (fixed) or dynamic to always achieve maximum (or minimum) common brightness between projection modules	
ICCC/TR/4.16		Fine-tune colour of each cube	
5. Monitoring Workstations			
ICCC/TR/5.01	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) / intel i7 or better	
ICCC/TR/5.02	Chipset	Latest series 64bit Chipset	
ICCC/TR/5.03	Motherboard	OEM Motherboard	
ICCC/TR/5.04	RAM	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC	
ICCC/TR/5.05	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)	
ICCC/TR/5.06	HDD	Minimum 2 TB SATA-3 or latest Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.	
ICCC/TR/5.07	Media Drive	No CD / DVD Drive	
ICCC/TR/5.08	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.	
ICCC/TR/5.09	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)	
ICCC/TR/5.10	Ports	Minimum 6 USB ports (out of that 2 in front)	
ICCC/TR/5.11	Keyboard	104 keys minimum OEM keyboard	
ICCC/TR/5.12	Mouse	2 button optical scroll mouse (USB)	
ICCC/TR/5.13	PTZ joystick controller (with 2 of the workstations in ICCC)	• PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered	
ICCC/TR/5.14	Monitor	22” TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified	
ICCC/TR/5.15	Certification	Energy star 5.0/BEE star certified	
ICCC/TR/5.16	Operating System	64 bit pre-loaded OS with recovery disc	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/5.17	Security	BIOS controlled electro-mechanical internal chassis lock for the system.	
ICCC/TR/5.18	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)	
ICCC/TR/5.19	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.	
6. Online UPS for field location			
ICCC/TR/6.1	Capacity	Adequate capacity to cover all above IT Components at respective field locations	
ICCC/TR/6.2	Technology	IGBT based PWM Technology, True Online UPS	
ICCC/TR/6.3	Input Frequency Range	45 to 55 Hz	
ICCC/TR/6.4	Output Frequency Range	45 to 55 Hz	
ICCC/TR/6.5	Output Voltage	220VAC -	
		230VAC	
ICCC/TR/6.6	Voltage Regulation	+/-2% (or better) and with built- in Over Voltage Cut off facility in the Device	
ICCC/TR/6.7	Frequency	50 Hz +/- 0.1% (free Run Mode)	
ICCC/TR/6.8	Harmonic Distortion (THD)	< 3% (linear load)	
ICCC/TR/6.9	Output Waveform	Pure Sine wave	
ICCC/TR/6.10	Output Power Factor	0.8 or more	
ICCC/TR/6.11	Battery Backup	Adequate and required battery backup to achieve required uptime of field device as well as SLA of the overall solution.	
ICCC/TR/6.12	Battery Type	Lead acid, Sealed Maintenance	
ICCC/TR/6.13	General Operating Temperature	As per City requirement	
ICCC/TR/6.14	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection	
ICCC/TR/6.15	Bypass	Automatic, Manual Bypass Switch	
ICCC/TR/6.16	Certifications	For Safety & EMC as per international standard	
ICCC/TR/6.17	Overall Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment 's and should also avoid intentional water splash and dust intake	
7. Online UPS for indoor location			
ICCC/TR/7.1	Capacity	Adequate capacity to cover all above IT Components at respective location	
ICCC/TR/7.2	Output Wave Form	Pure Sine wave	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/7.3	Input Power Factor at Full Load	>0.90	
ICCC/TR/7.4	Input	Three Phase 3 Wire for over 5 KVA	
ICCC/TR/7.5	Input Voltage Range	305-475VAC at	
		Full Load	
ICCC/TR/7.6	Input Frequency	50Hz +/- 3 Hz	
ICCC/TR/7.7	Output Voltage	400V AC, Three Phase for over 5 KVA UPS	
ICCC/TR/7.8	Output Frequency	50Hz+/- 0.5%	
ICCC/TR/7.9		(Free running);	
ICCC/TR/7.10		+/- 3% (Sync. Mode)	
ICCC/TR/7.11	Inverter efficiency	>90%	
ICCC/TR/7.12	Over All AC-AC Efficiency	>85%	
ICCC/TR/7.13	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short	
ICCC/TR/7.14	Battery Backup	60 minutes in full load	
ICCC/TR/7.15	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery	
ICCC/TR/7.16	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc.	
		Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.	
ICCC/TR/7.17	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.	
ICCC/TR/7.18	Cabinet	Rack / Tower type	
ICCC/TR/7.19	Operating Temp	0 to 50 degrees centigrade	
ICCC/TR/7.20	Management Protocol	SNMP Support through TCP/IP	
8. Desktop			
ICCC/TR/8.1	Make	Must be specified	
ICCC/TR/8.2	Model	Must be specified	
ICCC/TR/8.3	Processor	Intel Core i7-latest generation (3.0 Ghz) or higher OR AMD A10 7850B (3.0 Ghz) processor or higher OR Equivalent 64 bit x86 processor	
ICCC/TR/8.4	Memory	Minimum of 8 GB DDR4 RAM @ 2400 MHz. One DIMM Slot should be free for future upgrade	
ICCC/TR/8.5	Motherboard	OEM Motherboard	
ICCC/TR/8.6	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher	
ICCC/TR/8.7	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)	
ICCC/TR/8.8	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port	
ICCC/TR/8.9	Wireless Connectivity	Wireless LAN - 802.11b/g/n/	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/8.10	USB Ports	Minimum 4 USB ports (out of that 2 should be in front)	
ICCC/TR/8.11	Display Port	1 Display Port (HDMI/VGA) port	
ICCC/TR/8.12	Power supply	Maximum Rating 250 Watts, 80 plus certified power supply	
ICCC/TR/8.13	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.	
ICCC/TR/8.14	Mouse	Optical with USB interface (same make as desktop)	
ICCC/TR/8.15	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Should be TCO05 certified	
ICCC/TR/8.16	Operating System and Support	Pre-loaded appropriate 64 bit operating system with latest Windows / Linux Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. Can be downgraded to lower version like Windows Professional (64 bit) or Linux as applicable. All Utilities and driver software, bundled in CD/DVD/Pen-drive media	
ICCC/TR/8.17	Certification for Desktop	Energy Star 5.0 or above / BEE star certified	
ICCC/TR/8.18	Other pre-loaded software (open source/ free)	Latest version of Libreoffice, Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be preloaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.	
9. Laptop			
ICCC/TR/9.1	Make	Must be specified	
ICCC/TR/9.2	Model	Must be specified	
ICCC/TR/9.3	Processor	Intel Core i7 with latest generation or higher (OR) AMD A10 PRO 7300 (1.9Ghz) Processor or higher (OR) Equivalent 64 bit x86 processor	
ICCC/TR/9.4	Display	Minimum 15" Diagonal TFT Widescreen with minimum 1366 x 768 resolution (16:9 ratio)	
ICCC/TR/9.5	Memory	8 GB DDR3 RAM @ should be free for future upgrade	
ICCC/TR/9.6	Hard Disk Drive	Minimum 500 GB SATA HDD @ 5400 rpm	
ICCC/TR/9.7	Ports	• 3 USB Ports • 1- Gigabit LAN (RJ 45); • 1- HDMI/Display port, • 1- VGA, • 1- headphone/Microphone;	
ICCC/TR/9.8	Web Camera	Built in web cam	
ICCC/TR/9.9	Wireless Connectivity	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0	
ICCC/TR/9.10	Audio	Built-in Speakers	
ICCC/TR/9.11	Battery backup	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours	
ICCC/TR/9.12	Keyboard and Mouse	84 keys compatible keyboard, integrated Touch Pad.	
ICCC/TR/9.13	Operating System	Pre-loaded latest Windows/Linux Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		patches and updates. Can be downgraded to Windows/Linux (64 bit). All Utilities and driver software, bundled in CD/DVD/Pen-drive media	
ICCC/TR/9.14	Certification	Energy Star 5.0 or above / BEE star certified	
ICCC/TR/9.15	Weight	Laptop with battery (without DVD) should not weigh more than 2 Kg	
ICCC/TR/9.16	Accessories	Laptop carrying Back-pack. It should be from same OEM as laptop	
ICCC/TR/9.17	Other pre-loaded software (open source/ free)	• Latest version of Libre-office, Latest version of Adobe Acrobat Reader. • Scanning Software (as per scanner offered), this software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.	
10. Network colour Laser Printer			
ICCC/TR/10.1	Make	Must be specified	
ICCC/TR/10.2	Model	Must be specified	
ICCC/TR/10.3	Print Speed	Black : 15 ppm or above on A3, 24 ppm or above on A4	
ICCC/TR/10.4		Color : 8 ppm or above on A3, 12 ppm or above on A4	
ICCC/TR/10.5	Resolution	600 X 600 DPI	
ICCC/TR/10.6	Memory	Min. 8 MB or more	
ICCC/TR/10.7	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes	
ICCC/TR/10.8	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray	
ICCC/TR/10.9	Duty Cycle	25,000 sheets or better per month	
ICCC/TR/10.10	OS Support	latest Windows/Linux	
ICCC/TR/10.11	Interface	Ethernet Interface	
11. Fixed Dome Camera for Indoor Surveillance			
ICCC/TR/11.1	Video Compression	H.264, H.265/MJPEG/ MPEG-4 or better	
ICCC/TR/11.2	Video Resolution	1920 X 1080	
ICCC/TR/11.3	Frame rate	Min. 25 fps	
ICCC/TR/11.4	Image Sensor	1/3” Progressive Scan CCD / CMOS	
ICCC/TR/11.5	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager	
ICCC/TR/11.6	Lens#	Auto IRIS 2.8-10mm	
ICCC/TR/11.7	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264, H.265 individually configurable	
ICCC/TR/11.8	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)	
ICCC/TR/11.9	IR Cut Filter	Automatically Removable IR-cut filter	
ICCC/TR/11.10	Day/Night Mode	Colour, Mono, Auto	
ICCC/TR/11.11	S/N Ratio	≥ 50 dB	
ICCC/TR/11.12	Auto adjustment + Remote	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
	Control of Image settings		
ICCC/TR/11.13	Wide Dynamic Range	True WDR up to 80 db	
ICCC/TR/11.14	Audio	Full duplex, line in and line out, G.711, G.726	
ICCC/TR/11.15	Local storage	MicroSDXC up to 32GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.	
ICCC/TR/11.16	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF, Profile S&G	
ICCC/TR/11.17	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption	
ICCC/TR/11.18	Intelligent Video	Motion Detection & Tampering alert	
ICCC/TR/11.19	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface	
ICCC/TR/11.20	Operating conditions	As per City requirement	
ICCC/TR/11.21	Casing	NEMA 4X / IP-66 rated & IK 09	
ICCC/TR/11.22	Certification	UL2802 / EN, CE ,FCC	
ICCC/TR/11.23	Power	802.3 PoE (Class 0) and 12VDC/24AC	
12. Video Conferencing Unit			
ICCC/TR/12.1	General	• The multipoint function be done using a common server running VMware based Appliance Virtualization Platform and support H.323 and SIP optionally supporting H.263 , H.264, H.265 , H.264, H.265 High Profile and H.264, H.265 SVC • The Multipoint Conference Server should support Advance Video Coding format when connecting to end points and should retain the same layout and CP options of minimum 15 CP on the display unit. • All components of the solution – the multipoint conference server and software, Management software, Scheduling, web access desktop client software, web collaboration plug and WebRTC client should be from the same OEM. • In a multipoint conference server support symmetric 1080p30 conferences should be available on day one. • The multipoint conference server should support be a Full high definition and should support 1080p30, 720p30 and 480p30 resolutions in continuous presence mode using H.264, H.265 and H.264, H.265 SVC. • The capacity of the multipoint conference the number of ports should be 30 ports@720p30 or	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		15ports@1080p30 and upgradable to 40ports@720p30 and 80ports@480p30 in the same server. • Features should be uniform across protocols used H.264, H.265 AVC, H.264, H.265 SVC and H.264, H.265 Hi Profile.	
ICCC/TR/12.2	Video multipoint feature	• For security during a multipoint conference, standard ITU protocol - H.235 standard AES encryption without impacting port capacity. • Each participant should support a video layout of their own choice • The infrastructure for Multipoint conference server should support a feature of allowing the ability to scale his own video for optimal display on PC and TV screens using DTMF. • The Video infrastructure should support H.239 standard for sending/receiving multiple streams of video and presentation content. The H.239 support should not cost additional conference ports supporting 1080p30 for presentation and should allow web collaboration plug in for annotation and white boarding and application sharing. • The Multipoint conference infrastructure should support unlimited conferences as per the capacity of the Video Infrastructure as per the resolution selected – 1080p30 , 720p30 and 480p30	
ICCC/TR/12.3	Video Multipoint Infrastructure	• In a Multipoint conference server the number of Continuous Presence participants that are seen should be 15 with aspect ratios of 16:19 should supported from 480p30 resolution onwards. • The capacity of the number of 480p30 ports should be to four times the number of 1080p30 ports • The video infrastructure should support transcoding at 1080p30, 72030 and 480p30.	
ICCC/TR/12.4	Conference Management	• The management capacity supported should expandable in the future to increase concurrent calls. • The Management should support 80 concurrent calls and 400 registrations.	
ICCC/TR/12.5	Audio Protocol	• Should Support AAC-LC, Opus, Siren14/G.722.1 Annex C, G.722, G.722.1, G.729, G.711.	
ICCC/TR/12.6	Video Protocol	• Should Support H.263, H.264, H.265, H.264, H.265 Hi-Profile, VP8.	
ICCC/TR/12.7	Main Video Resolution	• Should Support CIF, 4CIF, 240p, 352p, 480p, 720p, and 1080p.	
ICCC/TR/12.8	Presentation Video Resolution	• Should Support CIF, VGA and 1080p and frame rates of 30fps	
ICCC/TR/12.9	Security	• H.235 AES encryption for secure conferencing • PIN protected conferences • HTTPS	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• The Management tool should support secure certificates. • The system should support Transport Layer Security (TLS) for secure signaling when connecting to SIP devices • The Video Infrastructure should be able to connect both H.235 and SRTP based devices in the same Multipoint conference	
ICCC/TR/12.10	Moderator Control	• The system should support H.243 Chair control functions for conference management by a terminal endpoint. • The Moderator should have the rights to conference control using functions like invite, terminate conference, take or release chair control, mute, volume control, video layout change and block or unblock admission to a conference	
ICCC/TR/12.11	Data Support	• Should support H.239 and Duo-Video standards for sending/receiving multiple streams of video and presentation content without losing Video infrastructure port capacity.	
ICCC/TR/12.12	Video CP Layout	• The Video Infrastructure shall support video processing capabilities that allow each site to see other sites simultaneously with continuous presence in dynamically layouts.	
ICCC/TR/12.13	Video Infrastructure Interface	• The Video Infrastructure shall provide a complete 'conference control' interface browser to support all 'in call' management functions with drag and drop' manipulation of parties in the call and within screen layouts.	
ICCC/TR/12.14	Conference Management software	• Through Management load balancing and call routing rules the Video Infrastructure should support scaling to larger installations • Shall include a software based H.323 Management function. • Shall support advanced bandwidth management for calls between Management sub-zones and remote zones to ensure proper call access control to the TCP/IP network for H.323 calls. • Shall support H.450 Call Forward and Transfer Supplementary Services. • Shall support call forwarding options including: unconditional forwarding, forward - busy and forward - no answer, and forward when not registered. • Shall support real time monitoring • Shall support advanced call fall back to ensure call completion rates.	
ICCC/TR/12.15	Conference scheduling	• Scheduling Capacity: Minimum 80 concurrent calls • Should support Microsoft/Linux/Unix scheduling with email notifications to individual participants and web collaboration.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• Should be provided in order to control all system resources, reserve conferences, and provide ongoing conference, point to point call, and fault management functions, through Web portal • Should be able to send e- mail notification to all participants. • The Web based application portal should implement single sign-on, wherein the enterprise Directory is accessed for pass-through authentication from the Web based application portal. • The conference scheduling application should support Direct Inward Dial to scheduled meetings. • The conference scheduling application should be able to manipulate conference layouts via a "drag and drop" Web user interface at scheduling time or in real time when conferences are in session • The conference scheduling application should support intelligent and optimized real time resource allocation algorithm for Multipoint ports on the Video Infrastructure and dynamically reuse the allocated ports according to the actual terminal capabilities. • The conference scheduling application should support Lecture style conferences where the lecturer sees students in a continuous presence layout, and the students all see the lecturer in a single screen layout.	
ICCC/TR/12.16	Reports	The conferencing application should provide a reporting and statistics support which will enable the system administration generate the following graphical charts / reports: • Number of Multipoint calls records for the entire deployment • Number of Point to Point calls records for the entire deployment Calls Records per terminal • Number of gateway calls for the deployment • Number of Desktop calls • Multipoint calls records per specific Virtual Room.	
ICCC/TR/12.17	Availability	The conference scheduling application and network management application should support redundant deployment for high availability in case required.	
ICCC/TR/12.18	Other Features	• The conference scheduling system admin should have the ability to provision the following attributes per user / groups of users: - Time zone, Level of Video/Audio Services (HD, SD, Audio Only), - Location Preference in a distributed deployment, - Recording Policy, if recording server implemented. - Maximum Allowed Bandwidth for calls. - Maximum allowed participants per virtual room. • The Scheduling Application should support corporate address book.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• The conference scheduling application should support management, load balancing and resource reservation of multiple distributed Video Infrastructure Gateways and Gatekeepers. • The conference scheduling application should support Dial-in or Video Infrastructure auto-Invite (Dial-out) to terminals. • Both the Management and the Scheduling and Network Management software should be installed on single server.	
ICCC/TR/12.19	Desktop Conferencing	• Minimum 1000 web access client download / WebRTC clients for Laptops and 1000 clients for mobile devices. • Desktop connectivity to PCs /laptops through desk top client installed and be able to participate in an ongoing conference using PC web camera and audio facilities and devices like Apple iPad , IPhone and Android phones. • The solution provided should support email exchange. This desktop clients on the PC should be able to initiate H.239 data collaboration and participate or View video and H.239 with support for annotation over H.239 • The desktop client should control the remote camera when required. • Desktop PC users should be able to connect behind firewalls with configuration. • Desktop PC users should be able to conference controls like lock meeting, terminate meeting, invite participant, mute/un-mute, disconnect any participant. • The Desktop client should support Waiting room and Virtual room with support for full screen video on the desktop. • It shall be possible to receive resolutions of 1080p on desktop clients. • Each Desktop Client participant should have the ability to change between voice activated video switching mode and continuous presence mode on the fly. • The Desktop Client user interface should provide simultaneous views of the participants and H.239 data collaboration portions of the conference. The user interface should provide full screen views of the participants or H.239 data collaboration portion of the conference. • It shall be possible to annotate over the presentation. The annotations should be sent as part of the standard H.239 stream so it is visible on all other H.239 complaint endpoints (software or hardware) connected to the conference.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• The Desktop Client should include a native component that enables desktop client participants to text chat while in conference. • The Desktop Client user interface should provide a participant list showing which participants are currently connected to the conference and whether each participant can send and is sending audio, is sending video, can send/receive data and is sending data. • The desktop administrator should be able to provision a directory of room systems. This directory shall be available in the desktop client user interface to ease the process of inviting room systems. • o.The Desktop Client solution should be able to secure conferences via PINs/passwords. • p.The desktop client should support white-boarding and web collaboration.	
13. Teleconferencing System			
ICCC/TR/13.1	Teleconferencing System	The Teleconferencing System shall use a telecommunications channel to link people at multiple locations. All IP phones shall be IPv4 and v6 compliant.	
ICCC/TR/13.2		The Teleconferencing System shall be interactive to provide two-way communications.	
ICCC/TR/13.3		The Teleconferencing System shall have conference phone with speaker that delivers performance required for the application and area.	
ICCC/TR/13.4		The Teleconferencing System shall use an audio signal processor that serves as the platform for the teleconference to integrate with the room audio system and control system.	
ICCC/TR/13.5		The Teleconferencing System shall have feature set for SIP-based VoIP platforms.	
ICCC/TR/13.6		The Teleconferencing System shall reduce listener fatigue by turning ordinary conference calls into crystal-clear interactive conversations.	
ICCC/TR/13.7		The Teleconferencing System shall deliver high-fidelity audio from 160 Hz to 22 kHz.	
ICCC/TR/13.8		The Teleconferencing System shall capture both the deeper lows and higher frequencies of the human voice for conference calls that sound as natural as being there.	
ICCC/TR/13.9		The Teleconference phone shall feature a large multi-line high-resolution LCD display of at least 3”.	
ICCC/TR/13.10		The phone shall be able to store contacts with quick dial feature.	
ICCC/TR/13.11		The teleconferencing system shall have configurable software.	
ICCC/TR/13.12		The Teleconferencing System shall support network power (POE) or DC power supply.	
ICCC/TR/13.13		The Teleconferencing System shall support 10/100/1000 Ethernet network.	
ICCC/TR/13.14		The Teleconferencing System shall be operational in temperature as per City requirement	
14. Room Control System including Panel			
ICCC/TR/14.1		The boardroom and the operations room shall have their independent room control systems. All systems including	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
	Room Control System including Panel	shadowing, lighting, HVAC, audio etc. being provided as part of the ICCC shall be integrated using this room control panel.	
ICCC/TR/14.2		The room control systems shall support a minimum of 7" touch panel display.	
ICCC/TR/14.3		The touch panel displays shall support a resolution of 1920 x 1080.	
ICCC/TR/14.4		The touch panel displays shall be desk mount with a cradle.	
ICCC/TR/14.5		The touch panel displays shall be wireless.	
ICCC/TR/14.6		The touch panel interfaces shall be intuitive and easy to use.	
ICCC/TR/14.7		The touch panel displays shall support full battery operations.	
ICCC/TR/14.8		The touch panel displays shall support full motion video preview and monitoring.	
ICCC/TR/14.9		The room control processors shall support secure industry standard communication protocol.	
ICCC/TR/14.10		The room control processors shall support the required number of ports for connection with variety of device following contract documents.	
ICCC/TR/14.11		The room control processors shall support 10/100/1000 Base-T.	
ICCC/TR/14.12		The room control processors shall support Ethernet-controllable devices.	
ICCC/TR/14.13		The room control processors shall support automatic clock synchronization.	
ICCC/TR/14.14		The room control panels shall support control system synchronization.	
ICCC/TR/14.15		The room control panels shall support multi-level password protection.	
ICCC/TR/14.16		The room control panels shall support an easy to use browser based user interface.	
ICCC/TR/14.17		The room control system hardware shall be rack mountable.	
ICCC/TR/14.18		The room control systems shall integrate with other non-AV systems in the room. This includes and not limited to window coverings and lights in both the operations room and boardroom.	
ICCC/TR/14.19		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/14.20		The room control system shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
15. EPABX System			
ICCC/TR/15.1	EPABX System	● The EPABX should have facility to accept at least 10 PRIs and should scale up to 1000 extensions to support the mix of analogue, digital and IP phones. ● Server based IP-PBX - IPPBX (Hardware & Software) shall be provided in high availability configuration. - The system should support IP or SIP as well as TDM. The TDM can be supported through an external Gateway. ● Communication System should support Analogy, Digital, IP, SIP, phones & Wireless IP Phone. ● The IP PBX should be modular, expandable, embedded IP server-gateway/server based architecture, having UNIX or Linux or equivalent operating system software based platform. ● The system shall have hot standby/Active-Active arrangement so that it should continue to operate in case of failure or maintenance of main processor or power	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		supply or interfacing card or CPU etc. The system should support IP or SIP as well as TDM. The TDM can be supported through an external Gateway. ● Support for ACD Call Center with CTI and advance call routing ● The system shall be able to provide following features like Basic Call Setup, Name and Number Support, Transit Counter, called or Calling or Busy or Connected Name and Number, Name Identification, Diversion (Call forwarding),Diversion (Call forwarding) with Reroute, Call transfer. ● It shall provide features as give below but not limited to these: - Call forward all, Call forward while busy, Call forward if no answer - Call hold , Call Drop and retrieve - Call Waiting and Retrieve (with configurable audible alerting) - Call Join - Call status (state, duration, number) - Conference for at least 5 parties - Missed call information on IP phone - Directory dial from phone - Hands-free, speakerphone - Last number redial - Malicious Call ID and Trace - Abbreviated Dial, Speed Dial	
ICCC/TR/15.2		ACD (Automatic Call Distribution) The key ACD features includes ANI/DNIS routing, managing multiple queues, welcome greeting messages, office hours configuration, standard and user defined reports, remote agent login, skill based routing, wait time notification, routing in incoming emails and web chat requests and integration with CRM, ticketing systems & voice logger ● ACD (Hardware & Software) shall be provided in high availability configuration. ● System should support skill base routing, multiple group support, priority handling and Queue status indicator. It is desirable that calls to certain trunk groups or to certain dialed numbers be assigned a higher priority than other calls and that calls which overflow from another split be queued ahead of other calls. ● The system should support call overflow routing e.g. if there is a queue in particular ACD group and another group is sitting idle, system should be able to transfer the calls to another group based on the settings defined by the administrator. ● The ACD should support help or assist on Officer's phone. Officer can use this functionality to request help from the split supervisor. This functionality automatically dials the split supervisor's extension and connects the Officer to the supervisor. Current call should go on hold as the Officer use this functionality.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• The proposed system should support the concept of virtual seating. Officers can log-on from any "soft phone" instrument within the system. Officers on the proposed system will be logically defined, rather than requiring a "soft phone" extension and termination. Each Officer on the system should have an individually assigned log- on identification number which permits individual statistics to be collected by the ACD management information system. • Automatic call distributor device should have capability to distribute the calls based on Skill level of the Officer like efficiency of the Officer and work load. • Automatic call distributor device should have functionality to provide best service to the caller like listen only, listen and talk only etc. • All calls for each ACD group (Skilled or Hunt) should be redirected to a different extension after hours. Supervisors should be able to activate this from their voice terminal. Each group may have different hours of operation. • Automatic call distributor device should provide alternate routing automatically based upon time of day and day of week. • Both Officers and supervisors should be notified via the telephone indicators when thresholds are reached for individuals and groups. • Calls can be queue to an individual Officer. Officer should be notified and a delay announcement be provided if the call queues for an individual Officer who is on another call. • Automatic call distributor device should support to force the Officers to be put into an ACW (After call work) state for a predefined period of time in order to provide rest time between calls, pace calls to the Officers, or limit the amount of time an Officer spends in completing wrap-up work. • Automatic call distributor device should be capable to define certain Officers as “reserve” Officers for certain skill sets which shall be able to handle call if configured incoming call threshold is exceeded. • ACD should be able to block nuisance callers against list of numbers captured in master database until either numbers is removed from the master database of nuisance callers. • In case of non-emergency, ACD System should allow auto transfer of calls to voice based feedback application which shall captures user’s feedback on multiple questions using DTMF inputs. • Automatic call distributor device should allow to change or add or remove Officer Skill dynamically while Officers are on calls. • System should allow an automation layer with different telephony and call control Java SDK’s	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		(Restful API's) in order to integrate with any 3rd party adjunct if required. ● The system should allow non-voice communication channel like email, web chat and SMS to be routed to Non-voice Officer based on skill set and Officer Availability. ● The System should allow Social Media Posts (from Facebook, Twitter) to be routed to non-voice officers as email and officer should be able to reply back which gets posted back on citizens' s Facebook / twitter message window. ● System should automatically inform the contact (via email) that their email has been received. ● System should be capable to distribute mails based on keywords in the subject or the body of the emails. Different rules can be used to route the mail to the right Officer or queue. ● User / Citizen should be able to do chat from Mobile App. ● The Web chat solution is required for users that prefer web chat as a medium to communicate with the Officer. ● An administrator should be able to configure the standard chat messages that will be presented during establishment of a chat session. The proposed solution is required for the users that prefer SMS as a medium.	
ICCC/TR/15.3		Self-Service IVR (Level-3 voice & text messaging) ● IVR should have self-help service with text to speech and automatic speech recognition. IVR should have flow designer with scripting capabilities, multi-language support. Interaction with uses using email, SMS (two way), and mobile web (visual IVR), customizable IVR prompts and agent greeting facility. IVR System ● IVR should support DTMF, speech recognition and Text to speech for Indian English, Odiya and Hindi languages. ● IVR should be support VXML. CCXML and MRCP. ● IVR should be able to pass caller entered information to ACD using CTI link. ● IVR should provide standard reports and custom reports built into the application. ● IVR should be able to support SMS and mobile web channels. ● IVR should be able to interact with caller with SMS or mobile web app while caller is on voice call. ● IVR should provide graphical user interface to create call flow / applications using drag and drop controls. ● Call Logger System - Voice recording system shall be provided in high availability configuration.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		- The recording software should use the recording interface provided by ACD or PBX API and should provide 100% voice call recordings. - The recording software should provide a single license that can support recording on all IP Phones. - The recording software should be able to record calls coming on any type of trunk line like PRI/IP and system should also record internal calls. - The software should record inbound calls and outbound calls. - The software should support for search and replay of calls. - The software should have Rules-based storage and recording. ● "Tag" or classify calls with user-defined labels for simplified search and replay. ● The software should support selective recording based upon user-defined business rules. ● The software shall be able to provide online, and offline storage capability in any combination. ● Should provide facility to store voice digitally in central database or to a hierarchical file system in any of the standard format like wav, mp3 etc. ● Archival to network attached storage or network drive should be included as a standard component with the recording platform. Recording of each call should be stored in the system. Recording should be available for citizen to download the file through citizen mobile application also.	
ICCC/TR/15.4		Call Center Communicator: The ICCC should be GUI based. It should include softphone, conference administration, pop-up agent works screen, unified interface for call handling, call transfer, call conference and missed call alerts. The ICCC should support Windows, Linux / Ubuntu operating systems.	
ICCC/TR/15.5		Real time agent monitoring: Should be provided with facility of barging, listening and monitoring calls.	
ICCC/TR/15.6		Voice Logger: There should provision of pre-integrated active voice logging, 100% blind recording, multi-format voice recording, automatic compression and archiving, remote access to voice logs. Quick and easy retrieval of recording file according to calls made and receive.	
ICCC/TR/15.7		Automation Platform a. Automation platform should allow citizens to interact with smart solutions such as smart parking & garbage collections. This platform should connect citizen engagement components such as IVR, chat bots, ACD to smart solutions to facilitate to and fro information. E.g. Citizen should be able to send SMS to check parking availability in the given area, IVR will use automation platform to connect to smart parking solution and retrieve the information and pass it to the citizen over SMS. The platform should also facilitate video streaming from the nearest video surveillance camera to the agent/ supervisor desktop when the caller is calling for an emergency by obtaining the location of the caller.	
ICCC/TR/15.8		Emergency Notification: The emergency notification system should be able to notify critical information to citizens using	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		audio, SMS and email based on target criteria such as location, demography of citizens. It should also be possible to broadcast pre-recorded audio, text message and a combination of these to all types of IP phones, IP speakers and broadcast paging system.	
ICCC/TR/15.9		Gateways: Centralized gateways shall route the calls received from any service provider to the command and control center through 4 PRI lines provision for inbound. Another 4 PRI lines need to be provisioned for outbound calls.	
ICCC/TR/15.10		Supervisor Application: There should be the facility of supervision on telephony, agent, dialer and lead performance, independent supervisor interfaces for inbound and outbound campaigns and complete MIS management for device, voice log, services & systems.	
ICCC/TR/15.11		Voice Recording and Storage: There should be facility of taking backups of system, agent, queue configuration automatically with time interval. Solution should provide graphical interface to maintain the storage location. The implementing agency will maintain the voice recording library. Incoming call recording facility to be implemented for further evaluation of complaints.	
ICCC/TR/15.12		CRM Module: CRM integration with IVR & ACD should be facilitated to enable customer profiling. Integration with any third party database, CRM or tool should be possible for seamless functioning and agent experience.	
ICCC/TR/15.13		CTI (Computer Telephony Integration Pop up) : • CTI pop-up shall appear on call takers desktop along with information of the caller (caller ID & address), which will help the call taker to call back in case of call disconnection. The application should be capable of integrating with other applications and scalable to meet the higher performance needs. The application should have capability to identify the caller location (for 2G/3G/4G phones with data connection). • CTI Application. • The CTI shall be capable of integrating with other application like CRM as per requirement. • The OS hosting the core CTI functionality shall be a flavor of UNIX or LINUX or Windows or any other supporting OS • The CTI link shall be able to pass events and information of Officer states and changes in Officer states as well as incoming calls to the computer applications, e.g.:- If the customer calls from the same no. from which caller had called earlier (registered Or unregistered), the CTI platform shall be able to automatically fetch and display at least last 5 service requests details for that customer. • In case of an abandoned calls, outbound COs should call back all abandon calls (within 600secs of call getting abandoned). • The System should offer web based application for sharing data (images, video) and location by caller to call center agents. Location tracking will be used for tracking caller location to very high accuracy by call takers to locate smart phone callers. • Automatic Call back: The automatic call back function would enable calling back the missed calls which	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		may be received on the system. It has to work in conjunction with the ACD as well. In case call disconnects while officer is speaking to caller, a notification should be presented to officer if it needs to be called back and if selected system should auto dial back the caller (without officer dialing a number manually).	
ICCC/TR/15.14		Phones: The MSI should provide standard digital or IP phones with 6 keys functional keys. It is advised to have an option to login to ACD from the phones in case CTI fails. This is considered as one of the redundancy features in the telephony. The phones should also have at least 6 part conference facility.	
ICCC/TR/15.15		Headphones for call responders The solution provider needs to facilitate the head phones with advance features for the call responders. It should have facility of own dial pad, volume control, flash button, tone/pulse dialing switch, last number redial button, mute button and over the head noise canceling functionality with clear sound clarity.	
ICCC/TR/15.16		Call Center Statistics The proposed solution should be able to provide real time statistics for agent/queue status, inbound & outbound call volume information in graphical format; data export in CSV & PDF format and should support windows & MAC operating system.	
ICCC/TR/15.17		**Reporting** ● The reporting system (hardware or software) shall be provided in hot standby configuration. ● The system shall provide both real-time information and historical reports. ● The system shall allow the user to set threshold on the Contact Center parameters, which shall be notified in the form of different colour on the screen of the users. ● There shall be provision to sort and filter the reports based on various criteria via date and time, Officer ID etc. ● Following category of real-time information & historical reports shall at least be available with specific dates and time with options of hourly, daily weekly and monthly, yearly in report criteria. - ACD Reports: Officer Login and Logout Reports. - Officer State Changes Report. - Queue Reports Abandon Call Reports. ● Call Details Report. ● Officer or Call taker Performance Reports: Average Hold Time per Officer or call taker, Average Call Handle Time per Officer, No. of calls handled per hour or per shifter Officer, Login & Logout duration per Officer. ● Call volume reports - number of calls during each hour, number of abandoned calls, number of incomplete calls, busy signals and rollovers, length of calls, percentage of calls answered and serviced vs. total calls received, etc.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• Provide details of calls in which the caller is placed on hold, using the following parameters: i. Hold time ii. Number of holds per call iii. Caller abandoned from hold iv. Officer or Call taker disconnected first. • The system shall provide Officers with the real time statistics on their desktop in form of a wallboard. Officers should get a notification if they exceed any pre-defined thresholds in form of a colour change on this wallboard. e.g. the wallboard display changes if a live call duration exceeds a threshold defined for calls. • Display call detailed reports including caller numbers, dialed number, call transfers etc. • It should be possible to archive or store certain data for more than one year. Such selected data could be electronically flagged to enable easy classification and then separate storage also. It shall have feature to schedule generation of reports and automatic delivery of scheduled reports to e-mail. It shall also allow automatic delivery of both manually generated and scheduled reports to a file directory or folder.	
ICCC/TR/15.18		Outbound System • The Outbound Solution should be an integrated part of the proposed ICCC. • The dialer should support outbound preview dialing, either automated or Officer-initiated. • The dialer should provide campaign management tool for supervisors to manage the campaigns. • The dialer should have the capability to fetch missed calls data from the ACD and dial out whenever the Officer is available. • The system should be able to perform a screen pop with caller information based on the campaign. • The system should be able to blast / dial out multiple calls and playback predefined announcements or sms static text or send emails. • The dialer should support campaign management for data selection. • The dialer should support Do not call list. Dialer should support agentless dialing.	
ICCC/TR/15.19		Emergency Notification System • The broadcasting solution is required for passing important and critical instructions to a group of citizen or users besides being used as a normal paging system. The broadcasting solution should be integrated with the call control system to enable IP Phone end points, to initiate a broadcast call/ message to IP Paging end point(s) / IP Phones. • It should support broadcast of pre-recorded audio, text messages, and a combination of these, to all types of IP Phones, IP Speakers and Broadcast paging system available. • It should be capable of creating different broadcasting group of recipients. It should possible	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		to add an IP Phone in two different broadcast groups. ● It should support scheduling of messages to be sent at a preset scheduled time or on a recurring basis. The duration of broadcast playback should be configurable. ● The system should be able to record all broadcasts of (pre-recorded audio) locally, with a provision to archive it on the network. The system should be able to send recorded voice message, SMS and email to the citizen based on location or demographic.	
ICCC/TR/15.20		IP Phone ● The IP phones with compatible wired headset should be supplied by the MSI. Headset should have echo cancellation. ● MSI should provide the soft phone for the desktop users. ● The IP Phone shall have an interactive and user-friendly alphanumeric display to make use of the key phone very simple. ● The IP Phone shall provide at least 6 programmable keys along with fixed feature buttons for Hold, Redial, Volume Up and Down, Mute, Hands free, Directory, Voice Message. There shall be possible to configure officer Login, Logout etc. ● The IP Phone shall include minimum two (2) port (100 /1000BaseT interface) switch for connecting PC or workstations. ● The IP Phone shall have LED or LCD Indicator for Call Waiting and Message Waiting. ● It shall be possible to create Local Phone book with at least 50 contacts as well as pull information from the directory (Integration with directory like Active directory Contact details etc.). ● The IP Phone shall support Voice Activity Detection, Silence Suppression and Echo Cancellation. ● The display shall provide features such as Date and Time, Calling Party Number and Digits Dialed. ● There shall be provision to provide electrical power to the IP phones through power adapter and via PoE (IEEE 802.3af) enabled Ethernet port. ● The IP phones shall support for POE Class 1 /Class 2 / Class3 ● The Phones shall have configurable Abbreviated Dial & Speed Dial. ● The firmware of IP phones shall be upgradable using HTTPS /FTP / TFTP/SFTP. ● It shall be possible to view call history for at least last 10 missed calls, 10 dialed calls and 10 received calls for each call taker desk. ● It shall be possible to set preferences such as Display Contrast and Ring Types.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		The IP Phones shall be SNMP manageable directly or through the PBX server. IP Phones or PBX server shall be able to send IP phone related SNMP traps to the configured Network Management System (NMS). MSI shall provide generic as well as vendor / OEM specific SNMP MIBs of the equipment for monitoring /management through standard NMS systems along with the equipment.	
16. Wireless Microphone Systems			
ICCC/TR/16.1	Wireless Microphone Systems	The wireless microphone shall be synchronized via RF remote channel.	
ICCC/TR/16.2		The wireless microphone shall be able to pick up audio from anywhere in the room, while maintaining quality audibility.	
ICCC/TR/16.3		The wireless microphone shall have a 24 MHz bandwidth (13 MHz for the E band).	
ICCC/TR/16.4		The wireless microphone shall have greater than 103 dB (A) signal-to-noise ratio.	
ICCC/TR/16.5		The wireless microphone shall have a Total Harmonic Distortion less than 1%.	
ICCC/TR/16.6		The wireless microphone shall support pick-up pattern applicable to table setup.	
ICCC/TR/16.7		The wireless microphone shall have frequencies tunable in steps of 25kHz.	
ICCC/TR/16.8		The wireless microphone shall incorporate a clip-on microphone and body pack.	
ICCC/TR/16.9		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/16.10		The wireless microphone shall use Radio Frequency for communication.	
ICCC/TR/16.11		The wireless microphone be operational in temperature as per City requirement	
17. Audio Processor			
ICCC/TR/17.1	Audio Processor	The audio processor shall have auto switching/mixing capability.	
ICCC/TR/17.2		The audio processor shall accept microphone and line level signals.	
ICCC/TR/17.3		The audio processor shall support external volume and mute control.	
ICCC/TR/17.4		The audio processor shall have balance and unbalance signals.	
ICCC/TR/17.5		The audio processor shall be able to rack mount, shelf mount on cabinet or under desk.	
ICCC/TR/17.6		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/17.7		The audio processor shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
18. Audio Distribution Amplifier			
ICCC/TR/18.1	Audio Distribution Amplifier	The audio distribution amplifier shall have balanced or unbalanced stereo or mono on a captive screw connector, unbalanced stereo or mono on RCA connectors and a 3.5 mm stereo mini jack.	
ICCC/TR/18.2		The audio distribution amplifier shall have an automatic clip limiter.	
ICCC/TR/18.3		The audio distribution amplifier shall have front panel bass, treble, and input level controls.	
ICCC/TR/18.4		The audio distribution amplifier shall be able to rack mount, shelf mount on cabinet, or under a desk as per design.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/18.5		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/18.6		The audio distribution amplifier shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
19. Audio Extractor			
ICCC/TR/19.1	Audio Extractor	The audio extractor shall be HDCP compliant.	
ICCC/TR/19.2		The audio extractor shall be capable of HDMI/DP audio de-embedding with analog stereo and digital S/PDIF audio outputs.	
ICCC/TR/19.3		The audio extractor shall be capable of de-embedding audio with/without HDMI/DP outputs connected.	
ICCC/TR/19.4		The audio extractor shall have simultaneous analog stereo and digital S/PDIF outputs.	
ICCC/TR/19.5		The audio extractor shall automatically equalize input cables.	
ICCC/TR/19.6		The amplifier shall be able to rack mount, shelf mount on cabinet, or under a desk.	
ICCC/TR/19.7		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/19.8		The audio extractor shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
20. Distribution Amplifier			
ICCC/TR/20.1	Distribution Amplifier	The distribution amplifier shall have HDMI or DP connector inputs conf.	
ICCC/TR/20.2		The distribution amplifier shall have at least two HDMI & DP connector outputs.	
ICCC/TR/20.3		The distribution amplifier shall be HDCP Compliant.	
ICCC/TR/20.4		The distribution amplifier shall continuously verify HDCP compliance.	
ICCC/TR/20.5		The distribution amplifier shall support computer-video to 1920x1200, including HDTV 1080p @ 60Hz and 2k.	
ICCC/TR/20.6		The distribution amplifier shall support HDMI& DP specification features including data rates up to 6.75 Gbps, deep colour up to 12-bit, Lip Sync, and HD lossless audio formats.	
ICCC/TR/20.7		The distribution amplifier shall equalize input cables automatically.	
ICCC/TR/20.8		The distribution amplifier shall have built-in scaling capability to match monitor display resolutions.	
ICCC/TR/20.9		The amplifier shall be able to rack mount, shelf mount on cabinet, or under a desk.	
ICCC/TR/20.10		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/20.11		The distribution amplifier shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
21. AV Auto Switcher			
ICCC/TR/21.1	AV Auto Switcher	The AV auto switcher shall have automatic switching capability between inputs.	
ICCC/TR/21.2		The AV auto switcher shall meet the minimum number of video and audio ports to support the design as a minimum. And additional 2 video and 2 audio ports for future connection.	
ICCC/TR/21.3		The AV auto switcher shall be capable of audio breakaway.	
ICCC/TR/21.4		The AV auto switcher shall have automatic scaling output and can support up to HDTV 1080p.	
ICCC/TR/21.5		The AV auto switcher shall have multiple digital and analog input.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/21.6		The AV auto switcher shall be HDCP compliant.	
ICCC/TR/21.7		The AV auto switcher shall be easily configurable with user friendly interface.	
ICCC/TR/21.8		The AV auto switcher shall be able to rack mount, shelf mount on cabinet or under desk.	
ICCC/TR/21.9		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/21.10		The AV auto switcher shall be operable between 0 and +40 °C / 10% to 85%, non-condensing.	
22. USB KVM Extender			
ICCC/TR/22.1	USB KVM Extender	The extender shall extend USB, keyboard, audio, video and mouse signals through a single cable CATx cable.	
ICCC/TR/22.2		The extender shall provide control on both the local and remote location. Controls include and not limited to video, keyboard, mouse and USB.	
ICCC/TR/22.3		The extender shall extend signals to a minimum distance of 300m via CATx cable.	
ICCC/TR/22.4		The extender shall automatically synchronizes the time delay of RGB signals to compensate for distance and support Auto Signal Compensation (ASC).	
ICCC/TR/22.5		The extender shall support high resolution video up to 1920 x 1200Hz (150 m); 1280 x 1024 at 300 m.	
ICCC/TR/22.6		The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
ICCC/TR/22.7		The extender shall support auto-negotiable 10/100/1000 Ethernet network.	
ICCC/TR/22.8		The extender shall be operational in temperature as per City requirement	
23. Contact Centre Solution (For Helpdesk)			
ICCC/TR/23.1	Contact Centre Solution (For Helpdesk)	The contact centre solution for Helpdesk shall include VoIP based EPABX, IVRS, Automatic Call Distribution (ACD), Voice Logger Server among other hardware and software. Using the contact centre solution, citizens can contact RSCL through the emergency communications system or through the contact centre helpline number.	
ICCC/TR/23.2		The contact centre solution shall be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call centre (s) along with interaction history of the calling party.	
ICCC/TR/23.3		The callers shall be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS). The information is envisaged to be available to the customer through telephone (IVRS) and call centres operators.	
ICCC/TR/23.4		The IVRS shall establish two way communication on the same channel with customers through recorded synthesized voice in Hindi / English / Oriya or in combination of languages to give information, reply to queries and provide other.	
ICCC/TR/23.5		IVRS shall be modular and scalable in nature for easy expansion without requiring any change in the software.	
ICCC/TR/23.6		It shall be possible to access IVRS through any of the access devices such as Landline telephone, Mobile phone (GSM as well as CDMA) etc.	
ICCC/TR/23.7		IVRS shall support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/23.8		The system shall have the ability to define business rules based upon which the system shall quickly identify, classify and prioritize callers, and using sophisticated routing, to deliver interactions to the best qualified operator in the any of the connected local/remote call centre, regardless of interaction channel.	
ICCC/TR/23.9		• The application shall provide (Computer-Telephony Integration) CTI services such as: • Automatic display (screen pop) of information concerning a user/customer on the call operator screen prior to taking the call based on ANI, DNIS or IVR data. • Synchronized transfer of the data and the call to the call centre operator. • Transfer of data corresponding to any query raised by any IP operator regarding a query raised by a customer whose call is being attended by the call IP operator. Call routing facilities such as business rule based routing, skills-based routing etc.	
ICCC/TR/23.10		The application shall support integration to leading CTI middleware vendors.	
ICCC/TR/23.11		It shall provide pre-integration with industry standard IVR servers and enhance routing & screen-pop by passing forward the information.	
ICCC/TR/23.12		It shall provide facilities for outbound calling list management, and software based predictive or preview dialing.	
ICCC/TR/23.13		The application shall allow service level plans to be varied by day, time of day, or a specific date.	
ICCC/TR/23.14		• Call Centre Operator's Desktop: The operators desktop shall have an application which shall fulfil the following functionalities: • It shall provide consistent operator interface across multiple media types like fax, SMS, telephone, email, and web call back. • Operator shall have VoIP based telephones (with digital display pads) on the workstation with wireless headsets. • It shall provide the operators with a help-desk functionality to guide the operators to answer a specific query intelligently. • It shall also provide an easy access to operators to previous similar query which was answered successfully. • It shall also be possible to identify a request to be a similar request made earlier. • It shall be possible for operators to mark a query as complex/typical and put in to database for future reference by other operators. • It shall be possible for operators to escalate the query.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/23.15		IVRS shall be able to get information /text/data from databases, convert to voice, and speaks it back to the caller in relevant/desired language.	
ICCC/TR/23.16		IVRS shall maintain log of all services offered which can be used for audit and analysis purpose.	
ICCC/TR/23.17		System shall provide for 100% recording of calls using a call logger. The recording shall contain detailed call information and the solution must provide advanced searching capabilities.	
ICCC/TR/23.18		There shall be enough provision for supervisory view supported by Supervisory terminals.	
ICCC/TR/23.19		System shall be able to integrate with e–mail / sms gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon.	
ICCC/TR/23.20		Shall intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to operators.	
ICCC/TR/23.21		Shall have an intelligent distribution of email to operators.	
ICCC/TR/23.22		• The contact centre solution shall support the following: • System shall be able to route emails to the Call agent using single system, based on the availability and skills and shall be able to send auto-acknowledgement. • System shall provide unified agent licenses to handle voice calls and emails. • System shall support auto-forward capabilities to pre-defined cell phone numbers i.e. auto patching. • System shall support single solution for inbound calls, outbound calls and emails handling and intelligently route the calls to available call agent.	
24. Building Management System			
ICCC/TR/24.1	General	Building Management System (BMS) shall incorporate industry standard operating systems, communication networks and protocols. The system shall be designed to be completely modular in structure and freely expandable at any stage.	
ICCC/TR/24.2		Overall system architecture shall be as following: • Management Level for system monitoring and management • System Level for intelligence of the system and data aggregation; and • Field Level for industry standard sensors, actuators, peripherals etc.	
ICCC/TR/24.3		Each layer of the system shall operate independently of the next level up, in order to allow for fault tolerant system functionality. Most importantly, the System Level shall operate independently without support from the Management Level.	
ICCC/TR/24.4		Building Management System shall consist of Administration and Programming Control Station, a family of Standalone Digital Control Units (SDCUs) consisting of field DDCs, field devices and sensors, BMS software and web-based	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		graphical interface. The BMS shall provide control, alarm detection, scheduling, reporting and information management for the entire facility as specified in this bid document.	
ICCC/TR/24.5		BMS shall consist of an Enterprise Server, which enables multiple DDCs (including all graphics, alarms, schedules, trends, programming, and configuration) to be accessible from a single workstation simultaneously for operations and engineering tasks.	
ICCC/TR/24.6		For Enterprise reporting and robust reporting capability outside of the trend chart and listing ability of the Workstation, a Reports Generating Application shall be installed on a BMS computer	
ICCC/TR/24.7		The system shall be support BACnet/IP, LonWorks, and/or Modbus protocol.	
ICCC/TR/24.8	Standard Network Support	All DDCs, Workstation(s) and Servers shall be capable of residing directly on the Client's Ethernet TCP/IP LAN/WAN with no required gateways. Furthermore, the DDCs, Workstation(s), and Server(s) shall be capable of using standard, commercially available, off-the-shelf Ethernet infrastructure components such as routers, switches and hubs.	
ICCC/TR/24.9	System Expansion	The BMS system shall be scalable and expandable at all levels of the system using the same software interface, and the same TCP/IP level and fieldbus level controllers. Systems that require replacement of either the workstation software or field controllers in order to expand the system shall not be acceptable.	
ICCC/TR/24.10		Web-Based BMS operation shall be supported directly by the DDCs and require no additional software.	
ICCC/TR/24.11		The system shall be capable of using graphical and/or line application programming language for the DDCs.	
ICCC/TR/24.12	Workstation Requirements	The control station shall support 30 days of recording of BMS data.	
ICCC/TR/24.13		Please refer to the Operator Workstation specification section.	
ICCC/TR/24.14	General Administration and Programming Workstation Software	System architecture shall be truly client-server in that the Workstation (Control Station) shall operate as the client while the DDCs shall operate as the servers. The client is responsible for the data presentation and validation of inputs while the servers are responsible for data gathering and delivery.	
ICCC/TR/24.15		The workstation functions shall include monitoring and programming of all DDC controllers. Monitoring consists of alarming, reporting, graphic displays, long term data storage, automatic data collection, and operator-initiated control actions such as schedule and setpoint adjustments.	
ICCC/TR/24.16	Web based BMS Requirements	Any user on the network can access the system, using the following: • Internet Explorer 11 or better • Mozilla Firefox	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		• Google Chrome	
ICCC/TR/24.17	User Interface	The operator panel on a workstation shall provide the primary interface for operator access to the BMS while also providing a tool for the annunciation of alarms and the reporting function. The operator shall have the option of switching between a text based and graphic based user interface at any time. Additionally, it shall be possible to create customized workspaces that can be assigned to user groups.	
ICCC/TR/24.18	User Security	The software shall be designed so that each user of the software can have a unique username and password. This username/password combination shall be linked to a set of capabilities within the software, set by and editable only by, a system administrator.	
ICCC/TR/24.19		The sets of capabilities shall range from View only, Acknowledge alarms, Enable / disable and change values, Program, and Administer. The system shall allow these capabilities to be applied independently to each and every class of object in the system. The system shall allow a minimum of 10 users to be configured per workstation.	
ICCC/TR/24.20	Help Facility	Software shall be provided to facilitate programming and storage of the system operation manuals in the hard-disk. The operation manual shall be retrieved by Online Help mode so as to enable the operator to self-learn the system operation, command, or function as and when needed.	
ICCC/TR/24.21		The facility shall contain both text and graphics to provide information about the selected function directly.	
ICCC/TR/24.22	Alarms	The software shall be capable of accepting alarms directly from controllers, or generating alarms based on evaluation of data in controllers and comparing to limits or conditional equations configured through the software. Any alarm (regardless of its origination) shall be integrated into the overall alarm management system and shall appear in all standard alarm reports, be available for operator acknowledgment, and have the option for displaying graphics, or reports.	
ICCC/TR/24.23		Multiple priority levels of alarm shall be made available. Priority levels shall be deemed Critical Alarms and Non-critical (general) Alarms. Critical alarms shall take precedence over non-critical alarms, and high priority over low priority under normal operations.	
ICCC/TR/24.24		It shall be possible to automatically provide details on alarms to authorized users via emails and SMS facilities.	
ICCC/TR/24.25	Logging	It shall be possible to log the status or value of system points at regular intervals or on change of state and store this on hard-disk at any of the workstation.	
ICCC/TR/24.26		It shall be possible to archive this information for future reference.	
ICCC/TR/24.27	Report Generation	Standard reports shall be provided that shall be operator selectable to appear on the operator workstation and any selected printer on the network.	
ICCC/TR/24.28		Each report shall be capable of being automatically	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		viewed/emailed to a user/recipient in Microsoft Word, Excel, and/or Adobe .pdf format.	
ICCC/TR/24.29		Reports can be of any length and contain any point attributes from any controller on the network.	
ICCC/TR/24.30		Image management functionality shall be possible to enable the system administrators to easily upload new logos or images to the system.	
ICCC/TR/24.31		The utility profile shall display the total consumption, measured peak for the current period and the previous period.	
ICCC/TR/24.32		Report generation tool shall display trending information of various building operations.	
ICCC/TR/24.33	Data Storage	A history file capability shall be provided to allow automatic storage of certain records plus allow the operator to selectively direct critical real time system data and activity to a mass storage device for later recall and analysis.	
ICCC/TR/24.34		It shall be possible to access software packages so that the operator may format display or printouts in the form of: • Spread sheets • Bar charts • Curve plots	
ICCC/TR/24.35		History files shall be the source data for stored trend reports to be used for records and system analysis.	
ICCC/TR/24.36	Time Scheduling	There shall be real time clock facility to help in time scheduling. The scheduling feature shall not be dependent on a central database or an operator workstation.	
ICCC/TR/24.37		From the workstation, it shall be possible to configure and download schedules for any of the controllers on the network.	
ICCC/TR/24.38	Point History	For every analog and digital point in the system, point history shall be maintained.	
ICCC/TR/24.39		The system shall provide point history graphs for analog/digital points.	
ICCC/TR/24.40	Point Trend	BMS shall be capable of point trending.	
ICCC/TR/24.41		Trend samples shall be displayed in either tabular or graphical format. A minimum of eight trended points shall be able to be displayed concurrently on a graph or report.	
ICCC/TR/24.42	Totalization	For every digital point, the system shall be able to calculate: • Cumulative on-time • Cumulative off-time	
ICCC/TR/24.43		For every point, analog and digital, the system shall be able to calculate: • Cumulative time in alarm • Cumulative time overridden by operator • Cumulative time offline	
ICCC/TR/24.44	Audit Trail	The workstation software shall automatically log and timestamp every operation that a user performs at a workstation, from logging on and off a workstation to changing a point value, modifying a program, enabling/disabling an object, viewing a graphic display, running a report, modifying a schedule, etc.	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/24.45	Database Manager	BMS shall include a database manager to allow the data to be managed on an integral and non-redundant basis. It shall be able to make additions and deletions to database, without affecting the existing data.	
ICCC/TR/24.46	Web based BMS Operator Software	General: • Day-to-day operation of the system shall be accessible through a standard web browser interface, allowing technicians and operators to view any part of the system from anywhere on the network via an IP address or dedicated webpage. • The system shall be able to be accessed on site via a mobile device environment with, at a minimum, access to overwrite and view system values.	
ICCC/TR/24.47		Graphic Displays • The browser-BMS interface must share the same graphical displays as the Control Workstations, presenting dynamic data on site layouts, floor plans, and equipment graphics. The browser's graphics shall support commands to change setpoints, enable/disable equipment and start/stop equipment.	
ICCC/TR/24.48		Alarm Management • Through the browser interface, a live alarm viewer identical to the alarm viewer on the control workstation shall be presented, if the user's password allows it. Users must be able to receive alarms, silence alarms, and acknowledge alarms through a browser. If desired, specific operator text must be able to be added to the alarm record before acknowledgement, attachments shall be viewable, and alarm checklists shall be available.	
ICCC/TR/24.49	Direct Digital Controller (DDC)	**IP based Direct Digital Controller (DDC) Hardware Requirement** • All the controllers shall be UL listed and BTL certified supporting to BACnet Protocol, LonWorks or Modbus. In case, controller is not BTL certified, equivalent or higher certification shall be required. • The controllers shall support BACnet, LonWorks or Modbus (all) on native backplane. • DDC's shall have 20% as overall spare capacity & at least one spare of each type of port shall be provided.	
ICCC/TR/24.50		**Direct Digital Controllers (DDC) Capabilities** • Controllers shall combine both network routing functions, control functions, and server functions into a single unit. • Controllers shall provide the interface between the field control devices, and connect with the control station. • Controllers must be able to perform the following energy management functions as a minimum: - Time & Event programs - Holiday Scheduling	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
		- Optimum start and stop program - Night purge - Load reset - Zero energy band - Duty cycle - Enthalpy analysis and control - Run Time Totalization - Sequencing and Optimization - Exception scheduling • Each DDC must have the ability to serve out web pages containing the same information that is available from the WorkStation. The development of the screens to accomplish shall not require any additional engineering labour over that required to show them at the WorkStation itself.	
ICCC/TR/24.51		**BACNet Fieldbus and BACNet SDCUs** • Networking IP Network: All devices that connect to the WAN shall be capable of operating at 10 megabits per second or 100 megabits per second.	
ICCC/TR/24.52		**Field Input / Output Devices** • List of Field Devices BMS shall optimize the performance of the building systems based on the input from field sensors. Field sensors to be decided and installed as approved by the Client.	
ICCC/TR/24.53		**Enclosures and Panels** • Enclosures for Controllers and Electrical Panels: All the controllers shall be housed in Lockable Vandal proof boxes which shall either be floor mounted or wall mounted. These shall be free standing, totally enclosed, dust and vermin proof and suitable for the climatic conditions.	
ICCC/TR/24.54		**Data Communication** • The communication between IP controllers shall be via a dedicated communication network as per manufacturer's standards. Controller microprocessor failures shall not cause loss of communication of the remainder of any network. All networks shall support global application programs, without the presence of a host PC.	
ICCC/TR/24.55		**Testing** • All the certificates and test reports submitted shall be from UL/NABL approved labs.	
25. Smart Phones			
ICCC/TR/25.1	Technology	GSM	
ICCC/TR/25.2	Display Size	Minimum 4.8 Inches	
ICCC/TR/25.3	Display Type	LCD or Amoled Touch Screen	
ICCC/TR/25.4	Display Resolution (Horizontal x Vertical)	720 x 1280 or above Pixel	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/25.5	Display Resolution @ Pixel Density	250 or above Pixels per inch	
ICCC/TR/25.6	Response time of Touch Screen	less than 50 milliseconds	
ICCC/TR/25.7	Sunlight Readability	300 or above Nits	
ICCC/TR/25.8	Life of Touch Screen	One million or above million touches	
ICCC/TR/25.9	Multitouch Support	Yes	
ICCC/TR/25.10	Display Protection	Tempered glass	
ICCC/TR/25.11	Processor Core	QUAD CORE or above	
ICCC/TR/25.12	Processor Speed	1.2 GHZ or above GHz	
ICCC/TR/25.13	Operating System	iOS/Windows OS/ Android Nougat 7 or above. HTML, XHTML, HTML5 and CSS3 compatible web browser	
ICCC/TR/25.14	Chipset	Spreadtrum, Mediatek, Snapdragon, Qualcomm, Exynos, Kirin	
ICCC/TR/25.15	RAM Size	1.5 GB or above GB	
ICCC/TR/25.16	Internal Storage	64 GB or above	
ICCC/TR/25.17	Storage Expandability	Yes	
ICCC/TR/25.18	Rear Camera Resolution	Min 5 MP Mega Pixels	
ICCC/TR/25.19	Front Camera Resolution	Min 2 MP Mega Pixels	
ICCC/TR/25.20	SIM Card Slots	2	
ICCC/TR/25.21	Type of Sim	Micro/Nano	
ICCC/TR/25.22	Connectivity	Support all GSM bands available in India with 2G, 3G and 4G with VoLTE	
ICCC/TR/25.23	Wi-fi Connectivity	802.11b/g/n	
ICCC/TR/25.24	Bluetooth Connectivity	4.0 or higher	
ICCC/TR/25.25	SAR Value	Less than 1.6 Watt/kg	
ICCC/TR/25.26	BIS Registration	Yes	
ICCC/TR/25.27	Battery Capacity	2600 or above mAH	
ICCC/TR/25.28	Battery Backup Time	At least 12 hours (Micro USB charging point, max 4 hours for full charge Hour	
ICCC/TR/25.29	Weight (With Battery)	Less upto 200 grams	
ICCC/TR/25.30	Warranty	3 years comprehensive inclusive of battery Year	
ICCC/TR/25.31	Compatibility with Other Devices	Should be compatible with Biometric devices and Printers	
26. Tablets			
ICCC/TR/26.1	Connectivity	Wifi+Cellular	
ICCC/TR/26.2	Operating System	Latest stable version of Android / IOS / Windows	

S. No.	Parameter	Minimum Technical Requirements	Compliant (Yes / No)
ICCC/TR/26.3	Display Size	7≤ N < 8 Inches	
ICCC/TR/26.4	Display Resolution	1024 x 600	
ICCC/TR/26.5	Display Type	LCD or TFT	
ICCC/TR/26.6	Sunlight Readability	400 or above Nits	
ICCC/TR/26.7	Processor	dual Core 1.2 GHz or above	
ICCC/TR/26.8	RAM Size	1.5 or above GB	
ICCC/TR/26.9	Internal Storage Capacity	64 GB or higher	
ICCC/TR/26.10	Rear Camera	4 MP or higher	
ICCC/TR/26.11	Front Camera	Not Mandatory	
ICCC/TR/26.12	Wi-Fi Connectivity	802.11a/b/g/n	
ICCC/TR/26.13	Bluetooth Connectivity	4.1 or above	
ICCC/TR/26.14	Weight	Less than 500 Grams	
ICCC/TR/26.15	Special Features	GPS; Music Player; Video Player; FM Radio; Accelerometer; Proximity sensor; Ambient light sensor; E-mail	
ICCC/TR/26.16	Battery	5000 mAH and above Lithium-ion Battery	
ICCC/TR/26.17	Accessories	• Power Adapter, Ear Phone with mike and all necessary accessories. • Tamper proof screen guard. Flip cover for the tablet	

Technical Requirements for ICCC: Non-IT Components

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
1. General Standards		
ICCC-NIT/TR/1.01	The ICCC interiors shall be state of the art adhering to the various best practices norms for integrated control centres, including: • Development of ergonomic reports for the ICCC covering Human Factors Engineering (HFE), • ISO9241 (Ergonomic requirements for office work with visual display terminals - VDTs) and • ISO11064 (Ergonomic Design of Control Centres) The proposed interior material should meet to basic control room norms, including but not limited to: • ASTM E84 or equivalent fire norms, • High scratch resistant surfaces, • Seismic zone compliance, and Green Guard passed Desk for ensuring safe environment for operators.	
2. Civil and Architectural Work		
ICCC-NIT/TR/2.01	• **False Ceiling (at ICCC)** - Metal false ceiling with powder coated 0.5mm thick hot dipped galvanized steel tiles of 595x595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanized steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	- 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners. • **Furniture and Fixture** - Workstation size of min. 18" depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc. - Storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1'6"x1'6"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish - Cabin table of min. Depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. - 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect. - Enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish. • **Partitions** (wherever required as per approved drawing) - Full height partition wall of 125 mm thick fireline gyp-board partition using 12.5 mm thick double fireline gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating. - With glazing including the framework of 4" x 2" powder coated aluminum section complete (in areas like partition between server room & other auxiliary areas). - Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this). - All doors should be minimum 1200 mm (4 ft.) wide.	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	• **Flooring** MSI shall procure and install a raised floor to match the floor height and room aesthetic in accordance with the approved final layout and design. MSI shall consider standard parameters for developing the final height, width, point of load, and uniform distribution load of the raised floor for the rooms based on type of furniture and overall load. MSI shall ensure the following features and parameters are considered while designing and commissioning the raised floor: - Point of Load (PoL) shall be considered 20% more than the actual load - Uniform Distribution Load shall be calculated according to the final Point of Load - Noise-proof, Fireproof - Maintenance window for easy access to under the raised floor - Separate electrical and data cable tray under the raised floor - Face of floor tiles shall conform to the aesthetic part of the approved design - MSI shall perform load test and noise test of the constructed raised floor. The MSI shall complete the following requirements for the raised flooring panels: - Floor shall be designed for standard load conforming to BIS 875-1987. - Panels shall be made up of 18-gauge steel of 600 mm × 600 mm size treated for corrosion and coated with epoxy conductive paint (minimum thickness 50 Micron). - Raised flooring covering shall be antistatic, high- pressure laminate, two (2) mm thick in approved shade and color with PVC trim edge. It shall not make any noise while walking on it or moving equipment. Load and stress tests on floor panels shall be performed as part of acceptance testing. • **Acoustic Requirements of Control room** - Control room being dead zone in acoustical terms, threshold should be lower than the normal. - Use of Acoustics and psychoacoustics measurements are must. Vendor to highlight the same in drawings. - Materials which define acoustics; it's the detailing which ensures controlled reverberations & resonances and reflections. • **Painting** - Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint. - For all vertical Plain surface. - For fireline gyp-board ceiling. - POP punning over cement plaster in perfect line and level with thickness of 10 – 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc. - Fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.	
3. PVC Conduit		

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
ICCC-NIT/TR/3.01	• The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983. • All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables. • No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit. • All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly. • Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes. • Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal. • The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.	
4. Wiring		
ICCC-NIT/TR/4.01	• PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Colour code for wiring shall be followed. • Looping system of wring shall be used, wires shall not be jointed. No reduction of strands permitted at terminations. • Wherever wiring is run through trucking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit. • Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply. • Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	• All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed. • Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap. • All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a mild steel sheet enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one. • Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.	
5. Earthing		
ICCC-NIT/TR/5.01	All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed. • Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, and A.C units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits. • All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded. • The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment. • Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm. • The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room. • There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data. • The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	• A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit need to be in place for this copper mesh. • Provide separate Earthing pits for Servers, UPS & Generators as per the standards.	
6. Cable Work		
ICCC-NIT/TR/6.01	• Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated. • All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick standard strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run. • Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall. • Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section. • Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc. • Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type. • The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.	
7. Air-conditioning		
ICCC-NIT/TR/7.01	• Cooling Capacity as per the requirements at each of the control rooms • Compressor – Hermetically Sealed Scroll Type • Refrigerant – R 22 Type • Power Supply – Three Phase, 380-415 V, 50 Hz • Air Flow Rate – minimum 19 cu m / min • Noise Level - < 50 dB • Operation – Remote Control	
8. Access Control System		
ICCC-NIT/TR/8.01	The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. Access control shall be provided for entry / exit doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality: • Controlled Entries to defined access points • Controlled exits from defined access points • Controlled entries and exits for visitors • Configurable system for user defined access policy for each access point • Record, report and archive each and every activity (permission granted and / or rejected) for each access point. • User defined reporting and log formats • Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc. • Day, Date, Time and duration based access rights should be user configurable for each access point and for each user. • One user can have different policy / access rights for different access points.	
9. Fire Alarm System		
ICCC-NIT/TR/9.01	• **System Description** - The Fire alarm system shall be a single loop addressable fire detection and alarm system, and should be installed as per NFPA 72 guidelines. - Detection shall be by means of automatic heat and smoke detectors (multi sensor) located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits. • **Control and indicating component** - The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of UL/EN54 Part 2 for the control and indicating component and UL/EN54 Part 4 for the internal power supply. - All controls of the system shall be via the control panel only. - The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display. - All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval. - The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command. • **Manual Controls** - Start sounders - Silence sounders - Reset system - Cancel fault buzzer - Display test - Delay sounder operation - Verify fire condition	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	- Disable loop • **Smoke detectors** – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of UL/EN54 Part 7. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base. - Heat detectors - Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point. - Devices shall be compatible with the CIE conforming to the requirements of UL/ EN54 Part 5 the detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base. - All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator. - The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. - Detector bases shall fit onto an industry standard conduit box. - Addressable Manual Call points should also be provided - Control & Monitor module should be provided for integration with 3rd party systems. • **Audible Alarms** – Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz. • **Commissioning** - The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.	
10. Rodent Repellent System		
ICCC-NIT/TR/10.01	The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace. Configuration: Master console with necessary transducer Operating Frequency: Above 20 KHz (Variable) Sound Output: 80 dB to 110 dB (at 1 meter) Power output: 800 mW per transducer Power consumption: 15 W approximately Power Supply: 230 V AC 50 Hz Mounting: Wall / Table Mounting	
11. Ceiling Speakers		
ICCC-NIT/TR/11.01	• The ceiling speakers shall have high power and high sensitivity with extended frequency responses. • The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.	

S. No.	Minimum Technical Specifications	Compliant (Yes / No)
	• The ceiling speakers shall have output of at least 15W peak. They shall have in-built amplifiers or shall be supported by an external amplifier. • The ceiling speakers shall have a conical coverage pattern. • The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design. • The ceiling speaker shall have a diameter not greater than 8.5". • MSI shall quantify and space speakers to provide full audio coverage within the command centre room and conference room. • The ceiling speakers shall follow the manufacturer recommendation for connectivity. • The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. This may require in-built noise sensors either with the ceiling speakers or with an independent ambient noise monitoring system.	
12. Miscellaneous		
ICCC-NIT/TR/12.01	• Conference table - Open type conference table for 08 people. Table top shall be of 25 mm thick Pre-laminated MDF board. - Legs: Ergonomically designed and matching with the open office concept. The leg is made out of specially designed aluminum extruded section. - Beam: Beam is made of heavy duty Extruded Horizontal Aluminum profile. - Cable tray: Shall be made up of 1mm thick CRCA sheet - Accessories: With POP Up Boxes Switch and Socket. • Shoe Rack: - Made up with 0.8 mm thick CRCA sheet powder coat finish/Pre-laminated Particle Board 18mm thick. • Coat & Helmet Stand made up of matt finish SS • Operator Chair:-High back executive chair with synchronized tilting mechanism with multiple locking systems, ABS for seat, mesh back with Silver Epoxy Backbone with extra lumber Support with fine tuning for depth adjustment, with four way adjustable armrest, gas lift for height adjustment, nylon base with castors. Upholstery: Black fabric seat & mesh backrest & Black Leatherite headrest • 3 Seater Sofa With Wooden Frame, SS Legs, Leatherite Tapestry Size (in mm) 1950 (L); 760 (D); 750 (H) • Printer Table for A4 size printer:- • Table top made of 25mm MDF. • Extruded aluminium profile with 2 mm thick. Vertical support. • Proper Cable tray for flow of wire.	

Helpdesk

MSI shall provide the operational support for all the locations, through a suitable helpdesk system, to ensure that the solution is functioning as intended and that all problems associated with operation are resolved satisfactorily during the contract period. The helpdesk will also provide facilities management services to support the Authority officials in performing their day-to-day functions related to this system. The MSI shall provide a web enabled helpdesk management system with SMS and email based alert system for the Helpdesk Call management and SLA reporting. MSI shall be required to setup a centralized helpdesk at two locations i.e. one at Command Control Center specifically for City Surveillance, and one at City Operation Center for rest of the solutions. The Central helpdesk should be dedicated (i.e. on premise) for the Project, which shall be supported

by their field units, proposed to be setup at Command & Communications Centers and various Viewing Centers. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted. Central Helpdesk should be set up at ICCC location.

The helpdesk management system should be fully integrated with the enterprise monitoring and network management system. The system will be accessed by the Authority officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the Successful MSI is required to maintain for provisioning of the Service Level Agreement of this RFP in Volume 3. Systems Integrator is also required to depute a dedicated, centralized project management & technical team for the overall Project management and interaction with Sr. Police Dept. personnel. Indicative resource requirement for this centralized administration of the Project is as follows:

MSI should setup

- Helpdesk at Integrated Command and Center for Operational Support
- Helpdesk for Citizens Emergency Call Button/Panic Button

MSI shall provision for the infrastructure necessary for managing the Help Desk including rent charges for Toll-free telephone line(s) at the Help Desk location. MSI shall provide multiple channels to log a complaint such as Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc. Outage of any component shall be calculated as a time between logging the call and closing the call.

A helpdesk is envisaged to be provided for the resolution of technical queries by internal users. Typical helpdesk activities (indicative) shall include, but not limited to:

- Deployment of sufficient manpower to attend the helpdesk requests for extending technical support on hardware, network, application etc. to users
- Deployment of web-based tool for the helpdesk
- Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through Toll-free lines, landlines, helpdesk tool, E-mail, direct walk-in etc.
- Implement a call logging system in line with the severity levels as per the SLAs. The Help desk shall log user calls related to system and assign an incident/ call ID number. Severity shall be assigned to each call as per the SLAs.
- Track each incident / call to resolution.
- Escalate the calls, to the appropriate levels, if necessary as per the escalation matrix agreed upon with RSCL/authorized entity
- Analyze the incident / call statistics and provide monthly reports including but not limited to:
    - Type of incidents / calls logged
    - Incidents / calls resolved
    - Incidents / calls open
- Helpdesk Solution shall further have the capability to upload frequently asked questions and solutions.
- The helpdesk should be integrated with Emergency Call box/Panic button that are installed across city.
- The Helpdesk application should be able to display the video from Emergency Call box/ Panic button, exchange the audio/video conversation with citizen.
- The helpdesk should route the call received by Emergency call box/Panic button to respective departments as specified by SOP for addressing the emergency call.
- The helpdesk should be logging the tickets and incident details received through Emergency call box/Panic button, the same is updated post routing the call to respective department.

Helpdesk becomes the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. This shall be the first level of support (L1).

The Helpdesk should be capable of transferring the call received to the respective departments such as fire department, police department, Healthcare. It shall also be capable of transferring the calls to any commercial establishments as per the call flow/SOP recommended by RSCL during implementation.

It is also expected that a second level of centralized support (L2) shall also be maintained at the same location from where the various zones/wards can be serviced in case of problem escalation. If a problem is not resolved by telephone/help desk tool and the User declares the problem to be of an emergency nature, MSI shall dispatch a Field Service Staff member who shall provide On-site Support Service according to service levels given.

The Helpdesk shall act as a single point of contact for all users whether for service requests, incidents or problems. It shall encompass Helpdesk, Asset Management and Vendor Management. In addition, it shall offer a focused approach for delivering integrated Service Management and provide an interface for other functions in IT Services Continuity Management like Maintenance Contracts, Software Licenses etc.

MSI shall implement effective Helpdesk Management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.

Helpdesk Capacity

MSI is required to provide helpdesk at Command Control Center during all operation hours as specified in the RFP. However, if the MSI believes that in order to meet the SLAs, additional capacity is required, the same may be provided by the MSI. It is also to be noted any supervisors required for the Helpdesk Operators shall be over and above the minimum operators mentioned above.

Shift Timings

The MSI shall operate the Central Helpdesk for the entire tenure of the Contract as follows:

Category	Shift	Type of Helpdesk Support	Type of Field Support
Helpdesk at Control Command Center for operational support	Shift 1	On-premise	On-call
	Shift 2	On-premise	On-call
	Shift 3 (night shift)	On-premise	On-call
Helpdesk for Citizens through Emergency Call Button/Panic Button	Shift 1	On-premise	Routing to Respective Department
	Shift 2	On-premise	Routing to Respective Department
	Shift 3 (night shift)	On-premise	Routing to Respective Department

Table 1: Shift Timings

Helpdesk Operators

The MSI is required to provide Operators at Helpdesk for operating and managing the Helpdesk as specified in this RFP. The Operators shall perform various activities including:

- Understanding the query/issue in the reported request. Query could be related to the following:
  - hardware including issues related to desktop/laptop, printer/multi-function device, local server, routers/switches
  - application including login and password issues, accessing a particular module, navigation assistance, report generation assistance
  - network including internet/intranet and end-user device connectivity
- Providing information / clarification on the spot in case of an informational query or providing necessary troubleshooting assistance in case of a logged issue
- In case of technical issues for which a resolution is not possible instantly, the operator shall submit the request into the system for escalation and further action by the MSI's team
- Process all service requests, dispatch them to field personnel who shall perform the follow up

Provision of the Operational Manpower to view the feeds at Command and & Communications Centers

Authority may ask the System Integrator to provide suitable manpower to monitor the feeds at Command and Communications Centers and support Authority in operationalization of the Command and Communications Centers. The exact role of these personnel and their responsibilities would be defined and monitored by Authority personnel. System Integrator shall be required to provide such manpower meeting following requirements:

- All such manpower shall be minimum graduate pass
- All such manpower shall be without any criminal background / record.
- Authority reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
- System Integrator shall have to replace any person, if not found suitable for the job.
- All the manpower shall have to undergo training from the System Integrator for at least 15 working days on the working of Command and Communications Centers. Training should also cover dos & don'ts and will have few.
- Sessions from Authority officers on right approaches for monitoring the feeds & providing feedback to Police Personnel / Surveillance System.
- Each person shall have to undergo compulsory 1 day training every month
- Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.
- Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.
- Authority reserves the right to include or exclude this scope of providing operational manpower in the Project scope or include it partly at the time of signing of the contract or during execution of the contract.

IT / Non IT Infrastructure for Helpdesk

The MSI shall be responsible for procurement, installation, commissioning and operations & maintenance of helpdesk including supply & installation of IT / Non IT infrastructure along with necessary application software (as per indicative BOM) required for the smooth functioning of the Central Helpdesk at both the location

Data Center and Disaster Recovery Center

Objective

The Data Centre will house the application and storage servers in the required secured environment. The Data Center will be co-located at the site identified for the ICCC. The Disaster Recovery Center is proposed at Bhubaneswar, which falls under a different seismic zone.

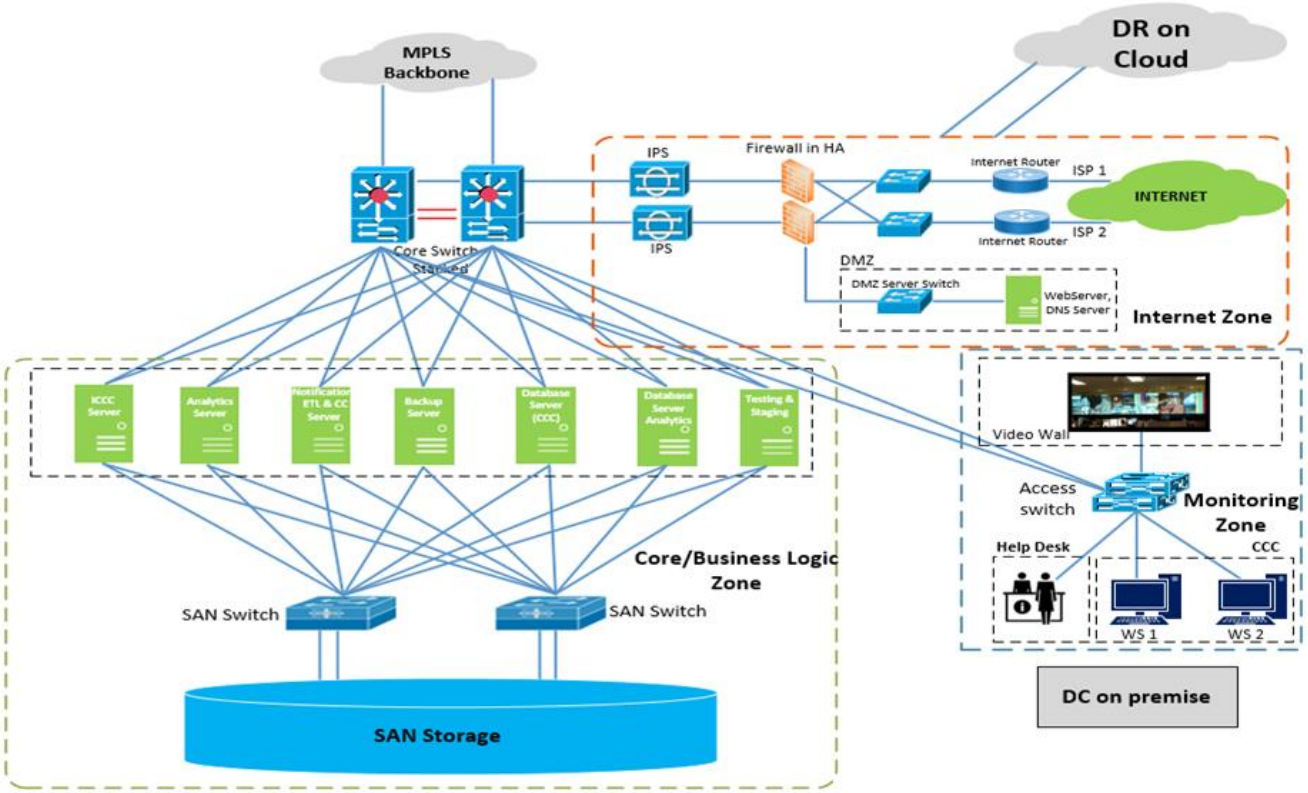
Scope of Work

The MSI shall ensure successful implementation of the proposed Data Center as per the scope of services described below:

- Data Center developed by MSI shall be as per Telecommunications Infrastructure Standard for Data Centers and shall satisfy the requirements for a Tier III data center
- Till the designated ICCC building is ready, the MSI shall setup a temporary Data Center at a space provided by RSCL. It shall be the responsibility of the MSI to migrate the temporary Data Center to the proposed ICCC building, once ready.
- The MSI shall prepare the overall data center establishment & its operational plan for this project. The plan shall comprise of deployment of all the equipment required under the project. The implementation roll-out plan for setting up the data center shall be approved by RSCL. The detailed plan shall be also comprise of the scalability, expandability and security that such data center shall implement under this project.
- The DR shall be located at Bhubaneswar and shall cater to minimum 10% load for replicating critical components with dynamic provisioning capability to handle 100% load in case of failures at data center.

Indicative Solution Architecture

The diagram below illustrates the key components/ solutions of the DC/DR. Please note that this component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of work and its intended use



The network architecture consists of various functional building block modules, with each module performing a set of specific functions. The architectural modules not only assist in the network design process, but also help in necessary IP address planning process. Further, the modules of the system serve as building blocks that are assembled into the larger DC network. The advantage of the modular approach is largely due to the isolation that it can provide. Failures that occur within a module can be isolated from the remainder of the network, providing for both simpler problem detection and higher overall system availability. Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation. The following Zones have been identified for the DC Network:

Intranet Zone
All the junctions, wards, Smart city elements, RMC offices will be connected to the data centre through the intranet zone. All the internal users can avail the data centre service through the intranet zone through the proposed backbone network (OFC). All video streams from the camera will pass through the intranet zone to the core/business logic zone.

Internet Zone
Internet routers are proposed in HA at DC extend services and deliver reliable connectivity to users coming via internet with a powerful blend of high-performance network protection and advanced services. All Internet traffic will be firewalled using Internet perimeter firewall and suitable policies will be enforced and the traffic would further be scanned through the IPS.

De-militarized Zone (DMZ): The purpose of a DMZ is to add an additional layer of security to an organization's network while the rest of the organization's network is firewalled.

Devices placed into the public DMZ could include the following:

- All publicly accessible web servers, including any front end database servers used by these web servers;
- All publicly accessible FTP or file servers;
- All publicly accessible collaboration servers;
- Web and email security firewalls (to be placed in front of the servers noted above);
- External DNS servers;
- Intrusion Detection/Prevention Systems (IDS/IPS)

MSI is expected to design the DC network in line with industry security best practices

Core/ Business Logic Zone
Core zone would control the application functionality by processing the business logic of the application. High performance and scalable core switch cluster has been provisioned in this layer. This layer would also have all the compute which will host applications & database in Data center. A unified architecture is proposed to provide dramatic reduction in network adapters, switches, and cabling.

Data Centre Requirements

Data Center Hardware and Software Components

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
1.	**DC Core /Aggregation Router**		
	Parameter	**Minimum Requirement**	
DCH/TR/1.01	Design and Architecture	• Chassis should have a minimum 6 x 1G SFP or more ports populated with Multi-mode transceivers. It should also support min 4 X10G interface on the same chassis for the redundant link and have support for T1/E1,V.35,STM interface. • The Fixed Router shall have integrated route processor, embedded services processor, and Interface modules and adaptors for future scale. Router should support a	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
		dedicated Processor for forwarding and encryption functions, independent of the Route Processor. • Router Processors should have minimum 1GB of internal memory to support multiple software images for backup purposes and future scalability . The router should support redundant routing engine with min 4GB of RAM. • The router should have min 60 GBPS throughput. • All modules, fan trays & Power supplies should be hot swappable and should support online insertion and removal. Shall have the support for redundant power supplies. • The router should be able to provide with 2 Operating System/redundant management module for bringing redundancy	
DCH/TR/1.02	Protocols	• Should support RIPv2, OSPF, IS-IS and BGP4 routing protocols, with support for all the features like OSPF on demand etc. & IP multicast routing protocols: PIM Version 2 (Sparse Mode & Dense Mode), IGMP v1, v2,v3 Should have support for protocols like Multiprotocol Label Switching (MPLS) & Virtual Route Forwarding (VRF)	
DCH/TR/1.03	Availability	• Should support dual images for redundancy. Should have modular software images, so that each software process runs independent of the other thus allowing for higher stability. Should also support online upgrade of patches for specific processes or ISSU without affecting traffic forwarding operations on the router.	
DCH/TR/1.04	Security	• The chassis should optionally support MD5 authentication for routing protocols. • The chassis shall function as a full fledge firewall & VPN concentrator upon activation of licenses. The router should optionally support IPsec encryption for data confidentiality. The router should optionally support 3DES and AES encryption standards with the activation of Security license. The Router should have min 4 GBPS of IPSEC through put.	
DCH/TR/1.05	Quality of Service	• The router should be able to support IP precedence and able to configure min. six classes of service. Should be able to do accounting based on IP precedence. • The router should support congestion management techniques like RED and Weighted Random Early Detection. • The router should support wide variety of queuing technologies like Weighted faire queuing, Low Latency Queueing etc.	
DCH/TR/1.06	Management	• Should support in-band and out of band management. • Should be able to support multiple Operating System images for smoother up gradation. • Should support fine-grained data collection including detail traffic statistics by protocol and IP address.	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
		• Services Processor/Module should additionally support the following functions in hardware & should be enabled using appropriate software license's only if required, without the need for additional hardware Interfaces Support : • Should support Fast Ethernet and Gigabit Ethernet, 10G Ethernet LAN support with ports in compliance with 802.3 standards. • Should be capable of supporting 802.1q VLANs and VLAN trunking. • Should support port aggregation for higher bandwidth and redundancy • Should support multimode and single mode fiber connectivity at Gig port	
DCH/TR/1.07	Performance	• Adapters holding interface modules should be optimized for high performance having a minimum of 1GB memory per interface module to support of large routing tables, rich Quality of Service features, and increased scalability.	
2	**Internet Router**		
	Parameter	**Minimum Requirement**	
DCH/TR/2.01	Design and Architecture	• Should be modular with 4 expansion slots and should have minimum 6 x 10/100/1000BaseT ports and 4 x 1G SFP ports • Should have 1 x 1G Out of Band Management ports, 1 x RJ-45 Console port and 1 x USB port • Should be provided with minimum 2GB DRAM and 512MB Flash memory • Should support T1/E1, VDSL and Serial Interfaces • Should have dual internal redundant power supplies	
DCH/TR/2.02	Performance Requirements	• Should support a Routing / Firewall multiprotocol forwarding throughput of minimum 5 Gbps, VPN throughput of 1Gbps and should support Min 1000 VPN tunnels • Should support a Route table size of minimum 500 K IPv4 / IPv6 Routes and support up to 256K concurrent IPv4/IPv6 sessions • Device should have all licenses required for Firewall, VPN, Switching & Routing functionality	
DCH/TR/2.03	Quality of Service (QoS)	• Should support Class-based queuing with prioritization • Should be possible to configure maximum bandwidth and guaranteed bandwidth • Should support Queuing based on VLAN, DLCI, interface, bundles, or filters • Should support Marking, policing, and shaping • Should support congestion management features like WRED	
DCH/TR/2.04	Routing protocol	• Should support IPv4 and IPv6 routing • Should support Min 600kpps of routing throughput • Devices should support RIP v1/v2, OSPFv2/v3, BGP and IS-IS	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
		• Should support MPLS (LDP), MPLS traffic engineering and MPLS fast reroute • The Device should support Policy Based Routing, Source Based Routing and ECMP • Device should support Virtual private LAN service (VPLS) and Multicast VPN • Device should support virtualization with virtual routers	
DCH/TR/2.05	Availability	• Should support VRRP • Should support stateful high availability with active/active dual box clustering • Should support firewall session synchronization • Should support on box monitoring with route and interface failover support • Should support Dial on-demand backup interfaces	
DCH/TR/2.06	L2 / L3 Feature	• Should support 802.1q VLAN with support for min. 64 VLAN • Should support Link Aggregation 802.3ad / LACP • Should support Jumbo Frames • Should support Spanning Tree Protocol (STP) 802.1D, RSTP 802.1w, MSTP 802.1s on all Ethernet ports • Should support 802.1x Port based and multiple supplicant authentication on all Ethernet ports • Should have an internal DHCP server • All Ethernet ports on the appliance should support full enterprise services including OSPF, BGP, PIM and IPv6 routing such as OSPFv3.	
DCH/TR/2.07	Multicast Features	• IPv4 Multicast features including IGMP v1/v2/v3 and PIM-SM, PIM-SSM and PIM-DM • Should support Session Description Protocol (SDP), Distance Vector Multicast Routing Protocol (DVMRP) & Multicast Source Discovery Protocol (MSDP),	
DCH/TR/2.08	Security Features	• Should have Stateful Firewalling with support for minimum 50 zones • Should support Network attack detection and support DDoS attack prevention • Should provide protection from protocol and traffic anomaly • Should have an Application Firewall with Application Visibility and Control • Should support a Group VPN Solution • Should support role of Group VPN server and provide support for maintaining security policies, authenticating the Group Members and providing the session key for encrypting traffic. This may be offered as integrated with VPN Concentrator or as a dedicated separate appliance • Should support SYN cookie protection and Zone-based IP Spoofing • Should support Network address translation (NAT) with support for Source NAT with PAT and Destination NAT with PAT, Persistent NAT and IPv6 Address translation	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
		• Should support for Intrusion Prevention System (IPS) with stateful signatures • Should support category and reputation based URL Filtering • Should support either an on box or cloud based solution for anti-malware protection by using a sandbox environment for detonating and observing threats • Should support inspection of .exe, .pdf and MS Office suite files including .doc, .ppt, .xls for anti-malware protection with detailed reporting • Should have provision to quarantine infected hosts and blocks communication	
DCH/TR/2.09	Management	• Should have Console, Telnet or Web for management • Should support Software upgrades through Web or CLI • Should support SNMPv2 and SNMPv3 and extensive debugs on all protocols • Should have flow monitoring and accounting services • Should have SLA monitoring features with support for Sessions, packets & bandwidth usage • Should support configuration rollback to a previous configuration • Should support data plane log export in Syslog • Should support scripting to allow for custom actions and commands based on specific user and environment needs	
3	**Smart Network iRack Specifications**		
	Parameter	**Minimum Requirement**	
DCH/TR/3.01	Type	19” 42U racks mounted on the floor meeting Tier 3 requirements. Standing Server Rack - 42U with Heavy Duty Extruded Aluminum Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. All racks should have mounting hardware 2 Packs, Blanking Panel. Stationery Shelf (2 sets per Rack) All racks should be lockable on all sides with unique key for each rack Racks should have Rear Cable Management channels, Roof and base cable access	
DCH/TR/3.02	Wire Managers	Two vertical and four horizontal	
DCH/TR/3.03	Power Distribution Units	2 per rack Power Distribution Unit - Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn. AC isolated input to Ground & Output to Ground	
DCH/TR/3.04	Doors	The racks should have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. Front and Back doors should be perforated with at least 63% or higher perforations. Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.	
DCH/TR/3.05	Fans and Fan	Fan Housing Unit 4 Fan Position (Top Mounted) (HA) - Monitored -	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Tray	Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor	
DCH/TR/3.06	Metal	Aluminum extruded profile	
DCH/TR/3.07	Side Panel	Detachable side panels	
DCH/TR/3.08	Management	Inbuilt power management, humidity control and fire suppression system and smart management of Rack for asset and monitoring	
4	**Authentication, Authorization and Access (AAA)**		
DCH/TR/4.01	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.		
DCH/TR/4.02	Should incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Should correlate and organize user, authentication, and device information together.		
DCH/TR/4.03	The solution Should be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform: • Built-in guest management and device/user on-boarding • Web based management interface with Dashboard • Reporting and analysis with custom data filters • Data repository for user, device, transaction information • Rich policies using identity, device, health or conditional elements • Deployment and implementation tools		
DCH/TR/4.04	The solution should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.		
DCH/TR/4.05	The solution should support captive portal customization, and even offers professional, in-house creation from day one		
DCH/TR/4.06	The Solution should support AAA, NAC and Guest Access		
DCH/TR/4.07	The solution should support the required number of endpoints as assessed by the MSI for AAA from day 1		
DCH/TR/4.08	The solution should support the required number of device profiles as assessed by the MSI from day one		
DCH/TR/4.09	The solution should be scalable and stable solution to support 2000000 endpoints for AAA in future using additional appliances		
DCH/TR/4.10	AAA server should have device profiling functionality for 25000 devices from day 1 to enforce context aware policies.		
DCH/TR/4.11	Solution should be Agnostic to existing wired, wireless and VPN network in place today.		
DCH/TR/4.12	Shell protected by CLI providing configuration for base appliance settings.		
DCH/TR/4.13	Appliance should provide disk or file encryption.		
DCH/TR/4.14	Ability to mix and match virtual and hardware appliances in one deployment.		
DCH/TR/4.15	Platform should be deployable in out-of-band model and support for clustering with N+1 active redundancy model.		
DCH/TR/4.16	Flexibility to operate all features/functions on any appliance in the cluster.		
DCH/TR/4.17	Server Cluster should be Upgradeable from the GUI. A single pane which upgrades all the nodes in a cluster		
DCH/TR/4.18	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.		

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/4.19	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).	
DCH/TR/4.20	Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).	
DCH/TR/4.21	Should incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Should correlate and organize user, authentication, and device information together.	
DCH/TR/4.22	Solution should have fully integrated support for Microsoft /Linux/Unix NAP allowing health and posture checks on Windows endpoints without the need to install an agent.	
DCH/TR/4.23	AAA server should support both functionality RADIUS server for client device authentication and TACACS+ for network device authentication and logging from day 1.Overlay component can be added to achieve both functionality.	
DCH/TR/4.24	The system should provide standard based external facing APIs to extend support and integration with external applications like Ticketing systems, Firewall, IDS/IPS solutions etc	
DCH/TR/4.25	The solution Should be an easy-to-deploy hardware platform that utilizes identity based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform: • Built-in guest management and device/ user on-boarding • Web based management interface with dashboard • Reporting and analysis with custom data filters • Data repository for user, device, transaction information • Rich policies using identity, device, health, or conditional elements • Deployment and implementation tools.	
DCH/TR/4.26	The solution should support flexible licensing model based on required functionality (i.e. Profile, Posture, Guest Access).	
DCH/TR/4.27	The solution should Correlation of user, device, and authentication information for easier troubleshooting, tracking	
DCH/TR/4.28	The solution should allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against Local database	
DCH/TR/4.29	The solution should support authentication or authorization support for LDAP, AD etc	
DCH/TR/4.30	Should support multiple methods for device identification and profiling	
DCH/TR/4.31	The solution should support endpoint audit	
DCH/TR/4.32	The solution should have policy creation tools: • Pre-configured templates • Wizard based interface • LDAP browser for quick look-up of AD attributes • Policy simulation engine for testing policy integrity	
DCH/TR/4.33	The solution should support the following enforcement methods: • VLAN steering via RADIUS IETF attributes and VSAs • VLAN steering and port bouncing via SNMP • Access control lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs • Roles Based Access or any other vendor-specific RADIUS attribute supported by the network device.	
DCH/TR/4.34	The solution should support Location Based Access	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/4.35	The solution should support Time Based Access	
DCH/TR/4.36	The solution should able to join multiple Active Directory domains to facilitate 802.1x PEAP authentication.	
DCH/TR/4.37	The solution should support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Should also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.	
DCH/TR/4.38	Failure of master node should not impact the ability for backup appliances to continue servicing authentication traffic.	
DCH/TR/4.39	Should support several deployment modes including centralized, distributed, or mixed.	
DCH/TR/4.40	The Policy Management solution should integrate with developed security and operations features like firewalls, MDM/EMM, and SIEM with REST based APIs , Syslog messaging, and deliver end-to-end policy enforcement and visibility from day 1	
DCH/TR/4.41	The solution should have Integrated Certificate Authority (CA) provides a complete and secure BYOD solution from day one	
DCH/TR/4.42	The solution should support for Single Sign On (SAML 2.0) and O-auth for social logins with Facebook, Twitter, Office365, GoogleApps, LinkedIn from day one	
DCH/TR/4.43	The solution should support a wide array of REST/SOAP/XML APIs and protocols that customers can use to integrate their own CRMs, helpdesks, SIEM vendors, admission systems and more from day one	
DCH/TR/4.44	The solution should support Cluster deployment provides High Availability (HA) solution with no touch automatic failover from day one	
DCH/TR/4.45	The solution should support multivendor solution for network access, supporting over 100 RADIUS vendor dictionaries for ultimate end-user flexibility from day one	
DCH/TR/4.46	The solution should consolidates all Policy Manager and license features into a single appliance or cluster	
DCH/TR/4.47	The solution should supports Profiling and MDM integration, in the base appliance, to gather endpoint attributes for policy enforcement from day one	
DCH/TR/4.48	The solution should support RADIUS/TACACS+ device administration from day one	
DCH/TR/4.49	The solution should support SQL as authentication source from day one	
DCH/TR/4.50	The solution should support HTTP enforcement (JSON, XML, HTTP payload) from day one	
DCH/TR/4.51	The solution should support Advanced Posture Health Classes for Windows and OSX like Disk Encryption, Virtual Machines, USB, P2P apps	
DCH/TR/4.52	The solution should support social Network SSO through O-Auth (Facebook, Twitter, Office365, Google Apps, etc.)	
DCH/TR/4.53	The solution should have Enhanced capabilities for endpoint compliance and control	
DCH/TR/4.54	The solution should supports Microsoft, Apple, Unix and Linux operating systems	
DCH/TR/4.55	The solution should support sponsored base Guest Access	
DCH/TR/4.56	The solution should support Self Provisioned Guest Access	
DCH/TR/4.57	The solution should maintain a list of active visitor sessions	
DCH/TR/4.58	Guest solution support a number of options for MAC Authentication and the ability to authenticate devices	
DCH/TR/4.59	Guest solution has ability to make changes to a visitor account's session while it is in progress.	
5	**Web Security**	
DCH/TR/5.01	• Should provide proxy, caching, content filtering, SSL inspection, protocol filtering, inline AV and content inspection in block mode on the same Appliance.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should support behavioral sandboxing to enhance advanced threat detection for Malware detection.	
DCH/TR/5.02	• Should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned security categories and vulnerabilities. • Should have real time content classification and security scanning with automatic database updates for security categories- Advanced malware command and control, Advanced malware payloads, Bot networks, Compromised websites, key loggers, Phishing and other frauds, Spywares	
DCH/TR/5.03	• Should inspect the sensitive content through 1500 pre-defined templates, textual content inside image, cumulative content control and inspection through web channel to prevent the content from being sent over outbound web channel. • Should have ability to provide geo-location awareness for security incidents. Should have ability to protect the sensitive data exfiltration based on geo-location.	
DCH/TR/5.04	• Should have min 20+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. • Solution vendor should ensure that 100 predefined categories & 100+ pre-defined protocols.	
DCH/TR/5.05	• Should support same policy enforcement in real time policy sync for users even when they access Internet outside the corporate network, this should be enforced through an agent deployment on roaming endpoints ((MAC and Windows - MAC OS X 10.10 and MS Windows 10) . • Solution should be on premises and not with the help of SAAS i.e. mobile user traffic should redirect to on premise solution for policy checks.	
DCH/TR/5.06	• Should have ability to block anonymizer sites or proxy avoidance tools. • Should be provided in default protocol database Ghost surf, Google web accelerator, Hopster, Jap, Real tunnel, Socks online, Tongtongtong, Toonel, Tor, Yourfreedom among others.	
DCH/TR/5.07	Should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below right from first day • Advanced Malware Command and Control category • Advanced Malware payload detection category • Malicious embedded links and iframe detection category • Mobile malware category • Key logger and Spyware category • P2P software database from day 1 to control/block the below P2P protocols	
DCH/TR/5.08	• Should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. • Should have social control video uploads to Facebook, Twitter, Instagram, YouTube and similar applications. • Should have built-in or custom policies for identifying and segregate You Tube traffic for education only and other irrelevant non-compliance video, • Should simplify design and implementation of policy to ensure user compliance	
DCH/TR/5.09	• Should provide geo-location awareness for security incidents.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should provide inbuilt capability malicious content of password and unknown encryption files. • Should support to have capability to differentiate between educational and entertainment videos through default categories and should have separate default categories for the same.	
DCH/TR/5.10	Should have visibility and blocking for cloud applications and shadow IT application usage for enhanced security.	
6	**Data Leakage Prevention (DLP)**	
DCH/TR/6.01	The solution should detect and prevent content getting posted or uploaded to specific websites, blogs, and forums accessed over HTTP, HTTPS. The solution should be able to enforce policies by URL's, domains or URL categories either natively or by integrated Web Security solution. The solution should be able to monitor FTP traffic including fully correlating transferred control information and should be able to monitor IM traffic even if it's tunneled over HTTP protocol.	
DCH/TR/6.02	The solution should be able to block outbound emails sent via SMTP if it violates the policy.	
DCH/TR/6.03	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.	
DCH/TR/6.04	The solution should be able to prevent content getting posted or uploaded to destinations (Web, Email domains etc.) and should monitor and control sensitive emails downloaded to mobile devices through ActiveSync.	
DCH/TR/6.05	The solution should support Email DLP deployment from any standard platform/OEM. All licenses required for the same should be included and management should be from the same centralized management platform.	
DCH/TR/6.06	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document. The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI.	
DCH/TR/6.07	The DLP Solution should natively monitor uploads as well as sharing of data from different assets connected outside the organization.	
DCH/TR/6.08	The DLP Solution should have capability to integrate with 3rd party Proxy solution for content inspection using ICAP channel or should have DLP engine on OEM provided Proxy itself.	
DCH/TR/6.09	The solution should Provide "Cloud Storage Applications" group which monitor sensitive content accessed by these cloud storage application on the endpoint and prevent sensitive data from uploading to the cloud. For Example (Should support from day 1(Windows 10 and MAC OSX 10.11) -Amazon Cloud Drive, Box, Drop box, Google Drive, Sky Drive, iCloud.	
DCH/TR/6.10	Endpoint solution should support win 32 and 64 bit OS, Mac & Linux OS, Support wide variety of platforms(Below support from Day1): Windows 7, Windows 8.1, and 10, Windows server 2008 R2, Windows server 2012 R2, Windows server 2012, Mac OS X -10.11.X,10.12.x, Red Hat Linux/Cent OS , VDI (Citrix and VM Ware)	
DCH/TR/6.11	The solution should Support PrtSc blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtSc capture will also be submitted to the DLP system as forensic evidence.	
DCH/TR/6.12	The Proposed DLP Solution should be GDPR Compliant.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/6.13	The solution should support the templates for detecting the Deep Web URLs- .i2P and .Onion , Encrypted attachments to competitors , Password Dissemination , User Traffic over time , Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.	
	End Point Data Monitoring & Protection	
DCH/TR/6.14	• The solution should have more than 50 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application. • The solution should be able to define the policies for the inside and out of office endpoint machines. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power or Machine is Idle.	
DCH/TR/6.15	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network. The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact and network components to reduce WAN overheads. The solution should be able to enforce different policies for desktops and laptops.	
DCH/TR/6.16	The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. The endpoint solution should encrypt information copied to removable media. It Should support both Native and Portable Encryption and manage the Encryption and DLP policies from the same management Console.	
DCH/TR/6.17	The solution should have ability to detect cumulative malware information leaks. The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns. The solution should able to detect and Block the sensitive information uploads to Group of P2P software: - Bit Tornado, Bit torrent, e Mule and e Mule Frost Wire.	
DCH/TR/6.18	The Endpoint DLP Solution should be able to encrypt data when business classified data is sent to removable media drives. The encryption solution can be built in or 3rd party solution needs to be factored to meet the requirement.	
DCH/TR/6.19	The Proposed Endpoint DLP Solution should be able to apply DLP policies to Microsoft RMS encrypted files on Windows endpoints to have better understanding of how RMS is being used by employees to protect sensitive data.	
DCH/TR/6.20	The solution should support the multiple Endpoint Profile Creation for the Better Security between the different departments. Encryption Keys are also should be isolated between the different departments. The endpoint installed should have the capability to create the Bypass ID after validation by the administrator by generating the Pass-code.	
	Data Identification & Policy Management	
DCH/TR/6.21	The solution should have a comprehensive list of pre-defined policies and templates with over 1700 patterns to identify and classify information pertaining India Information Technology Act, 2000	
DCH/TR/6.22	The solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and also the name of the file.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/6.23	The solution should be able to detect and block encrypted and password protected files without reading the encrypted content.	
DCH/TR/6.24	The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders.	
DCH/TR/6.25	The solution should be able to recursively inspect the content of compressed archives.	
DCH/TR/6.26	The solution should be able to fingerprint only specific fields or columns within a database and should be able to identify information from databases by correlating information residing in different columns in a database.	
DCH/TR/6.27	The solution should have printer agents for print servers to detect data leaks over print channel.	
DCH/TR/6.28	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	
DCH/TR/6.29	The solution should enforce policies to detect low and slow data leaks.	
DCH/TR/6.30	The solution should be able to enforce policies to detect data leaks even through image files through OCR technology.	
DCH/TR/6.31	The solution should be able to identify data leaked in the form unknown and known encrypted format like password protected word document.	
DCH/TR/6.32	The solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms.	
DCH/TR/6.33	The proposed DLP Solution should be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis.	
	Automated Response & Incident Management	
DCH/TR/6.34	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible.	
DCH/TR/6.35	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI.	
DCH/TR/6.36	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI.	
DCH/TR/6.37	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager.	
DCH/TR/6.38	The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator.	
DCH/TR/6.39	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	
DCH/TR/6.40	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.	
	Role Based Access and Privacy Control	
DCH/TR/6.41	The system should control incident access based on role and policy violated. The system should also allow a role creation for not having rights to view the identity of the user and the forensics of the incident.	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
DCH/TR/6.42	The system should create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint.		
DCH/TR/6.43	The system should allow a role only to view incidents but not manage or remediate them.		
DCH/TR/6.44	The system should have options to create a role to see summary reports, trend reports and high-level metrics without the ability to see individual incidents.		
DCH/TR/6.45	The system should allow incident managers and administrators to use their Active directory credentials to login into the console.		
	Reporting and Analytics		
DCH/TR/6.46	The solution should have a dashboard view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view.		
DCH/TR/6.47	The system should allow reports to be mailed directly from the UI and should allow automatic schedule of reports to identified recipients.		
DCH/TR/6.48	The reports should be exported to at least CSV, PDF, HTML formats.		
DCH/TR/6.49	The system should provide options to save specific reports as favourites for reuse		
DCH/TR/6.50	The system should have lots of pre-defined reports which administrators can leverage		
DCH/TR/6.51	The proposed solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console.		
DCH/TR/6.52	The Proposed DLP engine should perform a post-processing incident grouping step to avoid displaying related incidents in different cases. All incidents from the same user that have the same classification are combined into a group and DLP case card.		
DCH/TR/6.53	The DLP dashboard should display the number of cases in the designated period that fall above the risk score threshold that you've selected. Risk score thresholds should be customizable and instantly produce a report to prioritize the cases from high- to-low risk levels by leveraging analytics or machine learning technologies.		
	Storage (Data at rest)		
DCH/TR/6.54	The system should allow automatic movement or relocation of file, delete files during discovery.		
DCH/TR/6.55	The system should display the original file location and policy match details for files found to violate policy.		
DCH/TR/6.56	The system should leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes.		
DCH/TR/6.57	The system should support incremental scanning during discovery to reduce volumes of data to be scanned.		
	Management Monitoring		
DCH/TR/6.58	The solution should have centralized management and unified policy enforcement platform.		
DCH/TR/6.59	The solution should provide detailed reporting and if database is required for reporting then please provide hardware/software requirements for the same.		
7	**Blade Servers**		
DCH/TR/7.01	CPU	Intel CPU x86 of 8 Core or better	
DCH/TR/7.02	Form Factor	Blade Format	
DCH/TR/7.03	Processer Type	Intel	
DCH/TR/7.04	CPU Upgradeability	Up to 2 Nos. when required	
DCH/TR/7.05	No. of CPUs required currently	Min 8 cores using minimum 2 processor sockets	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
DCH/TR/7.06	The Memory in the proposed server should be DDR4	128 GB RAM using DDR4 Registered (RDIMM) memory and upgradeable up to 512 GB or more	
DCH/TR/7.07	Controller for this devices	SAS/SCSI/SSD	
DCH/TR/7.08	Total internal hard disk bays	2 Small Form Factor hot-plug SAS/SATA/SSD drive bays	
DCH/TR/7.09	Total disk capacity	2 x 1200 GB, 12Gbps SAS with 10K rpm or better	
DCH/TR/7.10	Ethernet	4 x 10 Gbps ports or batter and more as per network design	
DCH/TR/7.11	Management console Port	100 Base T Management LAN with web console access (with all additional licenses, if required)	
DCH/TR/7.12	PCI Slots	Each Server proposed should have minimum 2 PCI-E Slots or more	
DCH/TR/7.13	RAID features (support hardware or software RAID 0 & 1)	Must support RAID controller for RAID 0, Raid 1 configurations with 1GB Flash cache memory	
DCH/TR/7.14	Server Management	Support remote connection to LAN console port via SSH and web browser with SSL encryption LAN console port supports remote power up and power down control Support Event notification to system console	
DCH/TR/7.15	Management Indicator	Server should have LCD/LED indicators to identify System Health & failed components. System management should be through dedicated ports and should not use the adapters provided for the application	
	Server Management		
DCH/TR/7.16	Software should support dashboard view to quickly scan the managed resources to assess the overall health of the data center. It should provide an at-a-glance visual health summary of the resources user is authorized to view.		
DCH/TR/7.17	The Dashboard minimum should display a health summary of the following: • Server Profiles • Server Hardware • Appliance Alerts		
DCH/TR/7.18	Management software should support integration with popular virtualization platform management software like vCenter, and SCVMM		
DCH/TR/7.19	Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
DCH/TR/7.20	Should provide an online portal that can be accessible from anywhere. The portal should provide one stop, online access to the product, support information and provide information to track warranties, support contrast and status. The Portal should also provide a Personalized dashboard to monitor device heath, hardware events, contract and warranty status. Should provide a visual status of individual devices and device groups. The Portal should be available on premise (at our location - console based) or off premise (in the cloud).		
DCH/TR/7.21	Should help to proactively identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components.		
DCH/TR/7.22	The Server Management Software should be of the same brand as of the server supplier.		
DCH/TR/7.23	CPU:		

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	• Latest Generation x86-64 Bit Minimum 2.20 GHz with min. 10 Core and 16MB Cache or more. Processor should be from latest announced series • Offered Server should be configured with at least 2 Processors		
DCH/TR/7.24	Memory: Should be configured with 8 GB Per core RAM. Memory should be scalable to double the capacity configured		
DCH/TR/7.25	Memory Protection: Advanced ECC with multi-bit error protection, Online spare.		
DCH/TR/7.26	Hard disk drive with carrier: 2 * 600 GB hot plug SFF SAS drives.		
DCH/TR/7.27	Storage Controller: 12Gb/s SAS Raid Controller with RAID 0/1/1+0 and shall have at-least 1GB flash backed write cache.		
DCH/TR/7.28	Networking Features: Converged Network Adaptor with 40Gbps bandwidth i.e. 4 x 10Gbps or 2 x 20Gbps per downlink		
DCH/TR/7.29	Blade Server Connectivity to SAN: Should be capable of supporting 16 Gbps Dual port Fiber Channel HBA internal to the Server Blade.		
DCH/TR/7.30	Bus Slots: Minimum of 3 Nos of x16 PCIe 3.0 based mezzanine slots supporting Converged Ethernet/Ethernet/ FC adapters/SAS adaptors		
DCH/TR/7.31	Embedded System Management: • Should support Gigabit out of band management port to monitor the servers for ongoing management, service alerting and reporting. • Should support UEFI to configure and boot the servers securely • System should support RESTful API integration • System management should support provisioning servers by discovering and deploying 1 to few servers with embedded Provisioning tool • System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
DCH/TR/7.32	OS Support: • Microsoft Windows Server • Red Hat Enterprise Linux (RHEL) • SUSE Linux Enterprise Server (SLES) • VMware		
8	**Blade Chassis**		
DCH/TR/8.01	Form Factor	Server Chassis/Enclosure should be able to accommodate minimum 16 numbers of blades.	
DCH/TR/8.02	Blade Support	Should support Blade Servers of latest Intel Xeon based blades	
DCH/TR/8.03	RACK-U & Backplane	Should support Up to 10U chassis & Redundant backplane	
DCH/TR/8.04	Power Supplies	Must be configured for redundant power supplies, fans. Necessary PDUs to be provided. Power supplies, fans should be capable of reconfigure without manual intervention	
DCH/TR/8.05	Network Connectivity	• Should have redundant 10Gbps L2/L3 Ethernet switching to connect all the blades to the LAN and should be configured to minimize the no. of ports in the external • Should be minimum 2*10 Gbps uplink ports & 1G x 2 Ports from each 10Gbps switch to external LAN connectivity. • Should have support on enterprise L3 features supporting SDN,FC, FCOE,DCB & Scalable to support 40G when required • Shall be capable of increasing the number of NICs per connection without adding extra Blade I/O modules, and reducing cabling uplinks to the data centre network • Shall be capable of providing 10x10Gbps uplinks to connect to other Standard Data Centre Ethernet switches	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
DCH/TR/8.06	Management	• Each NIC shall be capable of tailoring the network bandwidth with their own dedicated, bandwidth per 10Gb downlink connection. • Min. 2 or more Physical/logical LAN ports for Virtualization • Should be configured with redundant hot pluggable management module to manage the blades using GUI • Should support simultaneous remote access of different servers in the chassis	
DCH/TR/8.07	Fiber Connectivity	Should provide Redundant fibre switches with minimum 16 ports each to connect server to external SAN switch	
DCH/TR/8.08	Availability	Each blade enclosure should have Cooling subsystem consisting of fully redundant hot pluggable fans or blowers. In case of failure the balance fans/ blower should ensure the smooth functioning of the blade system with all servers populated till the fan is replaced	
DCH/TR/8.09	DVD	Should have at least one DVD (R/W) drive per chassis (Internal/External)	
DCH/TR/8.10	Remote Management	Should provide support for remote console management, Power on/off blades, monitoring the power status, temperature, cooling fans status, I/O status, system diagnostic programs etc. provided through the management software.	
DCH/TR/8.11	Industries Compliance	Should support Ethernet/FC/ FCOE switches in blade chassis.	
9	**DC Core Switch**		
DCH/TR/9.01	Architecture • The Switch should support non-blocking Layer 2 switching and Layer 3 routing • There switch should not have any single point of failure like CPU, switching fabric, support module, power supplies and fans etc. should have 1:1/N+1 level of redundancy. • Switch support on line hot insertion and removal of different parts like modules/power supplies/fan tray should not require switch reboot and disrupt the functionality of the system • Switch should support the complete STACK of IP V4 and IP V6 services • Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied		
DCH/TR/9.02	Port / Module Requirement • Need to have 48 X 1G/10G Ports populated with following interfaces. - 12 x 1 G SFP; 12 RJ45 SFP & 18 Port SFP+ - 6 X 40GBE QSFP Fiber interface (Two wire Multi Mode/LC/ Two wire single mode- LC Fiber interface using OM4 minimum distance of 150 mtr)		
DCH/TR/9.03	Performance Requirement • Switch should support Min. 12,000 IPv4/IPv6 routes entries in routing table and should support at least 4,000 multicast routes or more • Switch should support Graceful Restart for OSPF, BGP etc. • Switch should support minimum 100 VRF instances or better • Switch should support up to 2.4 TBps of switching capacity including the services: - Switching - IP Routing (Static/Dynamic) - IP Forwarding - Policy Based Routing - QoS - ACL and Other IP Services		

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	- IP V.6 host and IP V.6 routing	
DCH/TR/9.04	Advance Features and Protocol support • Switch should support Python, NetConf, XML, Bash like services but not limited to. • Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S) • Switch should support basic Multicast IGMP v1, v2, v3 • Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. • Switch should support Jumbo Frames up to 9KB on 1G/10G Ports • Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities • Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures	
DCH/TR/9.05	Layer3 Features • Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface • Switch should support static and dynamic routing using: - Static routing - OSPF V.2 using MD5 Authentication - ISIS using MD5 Authentication - BGP V.4 using MD5 Authentication - Should support route redistribution between these protocols • Switch should recon verge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols • Switch should connecting multiple MPLS service provider using multi instance routing using VRF, VRF Edge routing and should support VRF Route leaking functionality • Switch should be capable to work as DHCP server and relay • Switch should provide multicast traffic reachable using: - PIM-SM - PIM-SSM - IGMP V.1, V.2 and V.3 • Switch should support Multicast routing of minimum 8 way Equal Cost Multi Path load splitting .However, the MSI shall do the required hard ware sizing	
DCH/TR/9.06	Quality of Service • Switch system should support 802.1P classification and marking of packet using: - CoS (Class of Service) - DSCP (Differentiated Services Code Point) • Switch should support for different type of QoS features for ream time traffic differential treatment using - Class- Based Weighted Random Early Detection - Strict Priority Queuing • Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x	
DCH/TR/9.07	Security • Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail • Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy • Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 • Switch should support for external database for AAA using: • TACACS and RADIUS • Switch should support DHCP Snooping, Dynamic Arp Inspection, IP Source Guard. • Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
DCH/TR/9.08	Manageability • Switch should support for embedded RMON/RMON-II for central NMS management and monitoring • Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail • Switch should provide remote logging for administration using: Telnet and SSH • Switch should support for management and monitoring status using different type of Industry standard NMS using SNMP v1,v2 and v3 • Switch should support Real time Packet Capture using Wire shark in real time for traffic analysis and fault finding • Switch should support central time server synchronisation using Network Time Protocol NTP V.4 • Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces • Switch should support for predefined and customised execution of script for device mange for automatic and scheduled system status update for monitoring and management • Switch should provide different privilege for login in to the system for monitoring and management	
DCH/TR/9.09	IPv6 features • Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as: - OSPF V.3 - BGP with IP V.6 - IP V.6 Policy based routing - IP V.6 Dual Stack etc. • Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode • Switch should support monitoring and management using different versions of SNMP in IP V.6 environment such as: - SNMPv1, SNMPv2c, SNMPv3 - SNMP over IP V.6 with encryption support for SNMP Version 3.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/9.10	Scalability • The Switch should support 1/10/40 G Scalable to 100G for future Scalability • The Switch should have minimum 4 Slots with min 2 free slot for future scalability. all the links configured should be in redundant configuration on two different cards in different slots	
10	**Access Switches**	
DCH/TR/10.01	Architecture: • Should support a minimum of 48 nos. 10/100/1000 Ethernet Ports • Should support a minimum of 4*10G SFP+ Uplinks • Should support 1G/10G trans receivers	
DCH/TR/10.02	Performance and Scalability • Should support Forwarding bandwidth of Min 100 Gbps • Should support Full-duplex Switching bandwidth of Min 200 Gbps • Should support 64-Byte Packet Forwarding Rate of Min 100 Mbps • Should support multi Core CPU • Should support minimum 128 MB of Flash memory • Should support minimum of 512 MB of DRAM • Should support 1000 Active VLANs • Should support Jumbo frames of 9K bytes • Should support up optimum number of Unicast MAC addresses and stacking	
DCH/TR/10.03	Stacking • Should enable all switches to function as a single virtual switch • Should support dedicated Stacking Port • Should be Hot-swappable • Should support a minimum of 5 Switches • Should support Min 50 Gbps of bi-directional throughput • Should support single IP address management for the group of switches • Switch proposed shall be compatible with any future upgradations/Models for the next min 5 years	
DCH/TR/10.04	PoE & PoE+ • Should support PoE (IEEE 802.3af) and 802.3at • Should support flexible power allocation across all ports • Should have 370W of Available PoE Power • Should support 24 ports up to 15.4W • Should support user configurable maximum PoE power per port • Should support reporting of actual PoE drawn per port	
DCH/TR/10.05	Power Supply: Should support an auto-ranging power supply for min power consumption and internal redundant Power supply	
11	**SAN Switch**	
DCH/TR/11.01	The switch should have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.	
DCH/TR/11.02	The switch should be able to support non-disruptive software upgrade.	
DCH/TR/11.03	The switch should be able to support process restart.	
DCH/TR/11.04	The switch should be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/11.05	The switch should be capable of supporting hardware-based routing between Virtual Fabric instances.	
DCH/TR/11.06	The switch should support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.	
DCH/TR/11.07	The switch should support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.	
DCH/TR/11.08	Inter-switch links should support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.	
DCH/TR/11.09	The switch should be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.	
DCH/TR/11.10	The switch should be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.	
DCH/TR/11.11	The fibre channel switch should be rack-mountable. Thereafter, all reference to the 'switch' shall pertain to the 'fibre channel switch'	
DCH/TR/11.12	The switch to be configured with minimum of 96 ports 16 Gbps FC configuration backward compatible to 4/8.	
DCH/TR/11.13	All 96 x FC ports for device connectivity should be 4/8/16 Gbps auto-sensing Fibre Channel ports.	
DCH/TR/11.14	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.	
DCH/TR/11.15	The switch should support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.	
DCH/TR/11.16	The switch should support routing between Virtual Fabric instances in hardware.	
DCH/TR/11.17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.	
DCH/TR/11.18	The switch should be able to load balance traffic through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID should also be supported.	
12	**Back-up Application**	
DCH/TR/12.01	The proposed Backup Solution should be available on various OS platforms such as Windows, Linux etc. and be capable of supporting SAN based backup / restore from various platforms including Linux, Windows etc.	
DCH/TR/12.02	The solution should offer centralized, web-based administration with a single view of all back up activities and should have alerts generation facility in case of any issue in backup process.	
DCH/TR/12.03	Support de-duplication at source and at target (disk) on any commodity storage volume. Based on policy backup software should be able to move data to a tape library automatically	
DCH/TR/12.04	Support scheduled unattended backup using policy-based management for all Server and OS platforms	
DCH/TR/12.05	Should have in-built frequency and calendar based scheduling system.	
DCH/TR/12.06	Should be able to backup any applications in online mode through online backup agents irrespective of the number of servers / CPUs, configuration of the servers , etc.	
DCH/TR/12.07	Should be capable of having multiple back-up sessions simultaneously	
DCH/TR/12.08	Should be capable of taking back up of SAN environment as well as LAN based backup.	
DCH/TR/12.09	Should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots	
DCH/TR/12.10	Should have the ability to integrate with archival software and create a single repository for backup and archive for space efficiency and easier data management.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/12.11	Should have in-built media management and supports cross platform Device & Media sharing in SAN environment.	
DCH/TR/12.12	Should be able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.	
DCH/TR/12.13	Should have online backup solution for different type of databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.	
DCH/TR/12.14	Should be able to copy data across firewall.	
DCH/TR/12.15	Should also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software should be capable of setting this utilization threshold for tapes	
DCH/TR/12.16	Should be able to support versioning and should be applicable to individual backed up objects.	
13	**Data Centre Firewall for Internet and Intranet (from different OEM)**	
DCH/TR/13.01	General • Should be a purpose built appliance based solution with integrated functions like Firewall, VPN and User awareness. The product licensing should be device based and not user/IP based (should support unlimited users except for VPN). The hardware platform & Firewall with integrated SSL/IPSec. • Should have minimum 70Gbps throughput. Throughput capacity of VPN under test conditions should not be less than 15 Gbps. • Should support Max 2,50,00,000 concurrent sessions for data. • Should support at least 1,80,000 connections per second. • Should be based on multi core processors and not on proprietary hardware platforms like ASICs, Should have minimum 16 GB memory with option of upgradable up to 32 GB. Hardware should have field upgradable capabilities for upgrading components like network cards, RAM, power supplies, fan etc. • Solution should have following deployment modes mandatory: a) L3 Mode, b) L2/Transparent Mode. • Should be deployed in High Availability. • Should support hardware fail open cards for critical interfaces. NGFW appliance should have inbuilt storage of 900 GB SSD / HDD. 8 x 10/100/1000Base-T Copper Ports, 4 x 10 GB 10G SFP ports from day 1 and support for addition of 2 x 40G SFP ports. Dedicated Management and Sync Ports	
DCH/TR/13.02	Firewall Feature: • Should be based on “stateful inspection” technology and should support access control for at least 500 predefined /services/protocols with capability to define custom services. • Shall allow security rules to be enforced within time intervals to be configured with an expiry date/time. • The communication between the management servers and the security gateways should be encrypted and authenticated with PKI Certificates.	
DCH/TR/13.03	Authentication • Support by the security gateway and VPN module: tokens (i.e. -Secure ID), TACACS, RADIUS and digital certificates. Should support Ethernet Bonding functionality for Full Mesh deployment architecture. • Should support user, client and session authentication methods. User authentication schemes should be supported by the security gateway and	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	VPN module: tokens (i.e. -Secure ID), TACACS, RADIUS and digital certificates. • Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously. Solution should support DCHP, server and relay. • Solution shall include the ability to work in Transparent/Bridge mode.	
DCH/TR/13.04	High Availability • Solution shall support gateway high availability and load sharing with state synchronization. • Solution shall support configuration of dual stack gateway on a bond interface or on a sub-interface of a bond interface. Solution should Support 6 to 4 NAT, or 6 to 4 tunnel.	
DCH/TR/13.05	User Identity / Awareness • Should be able to acquire user identity from Microsoft/Linux Active Directory without any type of agent installed on the domain controllers. • Should support Kerberos transparent authentication for single sign on. • Should support the use of LDAP nested groups. • Should be able to create rules and policies based on identity roles to be used across all security applications. • Should have the inherent ability to detect multi-stage attacks. • Should include static analysis technologies like antivirus, anti-malware/anti bot however in an integrate mode with the solution.	
DCH/TR/13.06	Security • Should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted. • The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. • Solution should have an ability to remove all the active content and macros sending only a clean document to the end user. • Solution should be able to detect & prevent the Bot communication with ICC. • Solution should have n Multi-tier engine to detect & prevent Command and Control IP/URL and DNS. • Solution should be able to detect & prevent unique communication patterns used by BOTs i.e. Information about Botnet family. • Solution should be able to detect & prevent attack types i.e., such as spam sending click fraud or self-distribution, that are associated with Bots. • Solution should be able to block traffic between infected Host and Remote Operator and not to legitimate destination. • Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malware type, Malware action etc.	
DCH/TR/13.07	The Log Viewer should have the ability view all of the security logs of all functions managed by the solution in one view pane (helpful when troubleshooting connectivity problem for one IP address)	
DCH/TR/13.08	The Log Viewer should have the ability in the log viewer to create filter using the predefined objects (hosts, network, groups, users...)	
14	**Application Delivery Controller (ADC) and Web Application Firewall (WAF) with Link Load Balancer**	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/14.01	Hardware & Performance • Should provide integrated functionalities of server load balancer, DNS, SSL and WAF. • Should provide 8 x 10G ports and 6 x 40G QSFP+ ports • Should support minimum SSL TPS of 80k (RSA 2k keys) and minimum 48K (with ECDSA 256 key). • Should support minimum 35 Gbps hardware based Compression throughput • Should support minimum 35 Gbps of SSL throughput • Should support minimum 2M DNS Query Per Second • Should support minimum 100 Million L4 connection	
DCH/TR/14.02	Availability • Should be able to load balance both TCP and UDP based application from L2 to L7 including lightweight MQTT protocol for machine to machine connectivity between IoT appliances such as small sensors, mobile devices etc. • Should be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, hardware based compression, caching etc. in active-passive mode. • Should offer out of band programming for control plane along with data plane scripting for function like content inspection and traffic management • Should support SQL-based querying for the following databases for health checks: Oracle, MSSQL, MySQL, PostgreSQL, DB2 • Should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover • Should support centralized Security policies enforcement, SSL Certificates management for workloads on Private DC and public cloud authorized by Government of India • Should support a mechanism to auto-discover and auto-scale workloads deployed in Public Cloud. • Should support global server load balancing between DC and on premise/cloud based DR • Should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration • Should support API protection • Should support Web socket and Secure Web socket • Should provide Link load balancing of min 4 internet links and should be scalable to support 16 internet links. • Should support policy nesting at layer4 and layer7 to address the complex application integration. Further it should also provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc.	
DCH/TR/14.03	Security • Should provide comprehensive security both at network and application level via WAF and SSL Virtual Private Network module on a single device. • Geolocation IP address database to identify the source of the attack origin and IP Reputation Mechanism to identify the Blacklisted TOR Networks or Proxy IP address to Block the request immediately. • Should have both positive and negative security model with machine learning capabilities to detect and prevent vulnerabilities and anomalies in application traffic and unknown attacks.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Machine learning should be based on true ML algorithms, and not just automation of dynamically learnt rules. • New/updated modules of applications should be learnt dynamically, and WAF should also provide the option of deploying the rules learnt dynamically for these new modules without manual intervention. • WAF correlation should also identify complex attack chains, and not just aggregate events based on attacks or sources along with advanced BOT detection mechanism based on smart combination of signature-based and heuristic analysis • Should be able to take threat intelligence feed to reveal inbound communication with malicious IP addresses, and enable granular threat reporting and automated blocking. • Should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration • Should be stable and not affect service availability even upon any system fault • System should be able to encrypt the user credentials in real time ,any other sensitive parameter as defined by department to protect from key loggers and credential stealing malware residing in the end users system • Should support SSL offloading using both RSA and ECC based keys • Solution should be able to detect the presence of Remote Access Trojans (RATs) residing in the user's web browser. • Solution should perform comprehensive countermeasure to protect against zero day attack, Challenge – Response Mechanism, which should be able to detect and protect attacks in real time through inbuilt Captcha Mechanism • Able to defend against browser based key loggers that attempt to capture user's key strokes and steal user credential • SSL VPN for remote user access and management with AD, LDAP, Radius and TACACS integration for authentication • Solution should integrate with AD, LDAP, Radius, TACACS with inbuilt OTP mechanism for 2 Factor Authentication	
DCH/TR/14.04	Management, Reporting • Should be manageable from a single management platform • Should support integration with SIEM and other Monitoring and Reporting solution	
15	**Advanced Persistent Threat**	
DCH/TR/15.01	Should be hardened appliance based on premise solution	
DCH/TR/15.02	Should provide a high performance architecture with comprehensive layered malware protection including Antivirus, Threat Intelligence, and Gateway Anti Malware and advance sandboxing all from a single OEM and should not be a combination from different OEM's	
DCH/TR/15.03	Should integrate with the proposed Advance Endpoint Protection solution along with the proposed Network IPS and Web Proxy solution in an automated manner.	
DCH/TR/15.04	Should be able to statically analyze the source code of the malware and perform true static code analysis and not just static file analysis.	
DCH/TR/15.05	Should identify any logic bombs hidden in the malware waiting for a trigger to cause damage at a later time.	
DCH/TR/15.06	Should provide broad Virtual Machine support: Sandbox analysis environment matches target and Analyze objects and executables with the applications on the following platforms: • Supports x32 and x64 Windows platforms	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Supports Windows Server and Desktop OS • Supports custom image creation • Android	
DCH/TR/15.07	Should be enterprise wide scalable and with the ability to handle up to 100,000 objects per day / per appliance.	
DCH/TR/15.08	Should provide for on premise based sandbox technology where the objectionable content may be executed and inspected	
DCH/TR/15.09	Should support at least 10 multiple simultaneous VM images for target specific Sandboxing to identify malware.	
DCH/TR/15.10	The proposed solution should be able to identify malware that has been packed or protected with Crypters, Packers.	
DCH/TR/15.11	Should support the following multiple advanced malware analysis methods: • AV Signature • Threat Reputation • Signature-less engine • Sandboxing • Static Code analysis • Dynamic Code analysis	
DCH/TR/15.12	Should provide the ability to upload and analyze objects through a collection of custom virtual machines rather than a generic image.	
DCH/TR/15.13	Should support down selection and only analyzes files deemed suspicious.	
DCH/TR/15.14	Should have the ability to heuristically detect and decode the presence of shell code	
DCH/TR/15.15	Should have the ability to detect and scan pdf files for embedded code	
DCH/TR/15.16	Should have the ability to unpack the code and remove any obfuscation to identify the original executable code.	
DCH/TR/15.17	Should recognize new variants of existing malware families and identify new families.	
DCH/TR/15.18	Should have capability to fully reveal malware's current and potential payloads.	
DCH/TR/15.19	Should provide detection, analysis and repair capability against malware-based attacks	
DCH/TR/15.20	Should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.	
DCH/TR/15.21	Should provide reports to shows all the activities the malware code performs related to file systems, Windows registry, network operations, Processes and any other miscellaneous operations	
DCH/TR/15.22	Should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific URL, or changed the name of a running process to hide itself.	
DCH/TR/15.23	Should identify any logic bombs (time based execution delays) hidden in the malware waiting for a trigger to cause damage at a later time	
DCH/TR/15.24	Should provide real-time intelligence about the behavior of the suspect code without requiring any signatures or updates from the vendor	
DCH/TR/15.25	Should provide the ability to upload gold image and analyze threats under conditions of actual host environment.	
DCH/TR/15.26	Should provide Detailed Technical Report, Behavior Summary Report and a Logic Execution Path Map.	
16	**NAS/SAN Storage**	
DCH/TR/16.01	General • Storage Solution with NSPoF (No single point of failure) Architecture.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should support NAS & SAN as an integrated offering with high availability at each level. • Should allow upgrades of hardware and software for investment protection.	
DCH/TR/16.02	Protocols: Solution should be configured with required protocols for the solution CIFS/SMB 3/ NFS 4/iSCSI/FC. All required protocols required for the solution to be enabled.	
DCH/TR/16.03	Controllers: Each controller shall be configured with minimum 10 core or higher CPU.	
DCH/TR/16.04	Operating System: Array should support all Operating System Platforms & Clustering including: Linux/Windows	
DCH/TR/16.05	Cache Memory: Should be provided with minimum 256 GB cache or more.	
DCH/TR/16.06	Host: Should be capable of providing host connectivity as per solution offered (Unified/SAN/NAS/Scale out NAS).	
DCH/TR/16.07	Connectivity: Minimum 2 ports per controller to be provided for host connectivity	
DCH/TR/16.08	RAID Supports: RAID levels Supported: Mirroring, Single parity, Dual parity or higher.	
DCH/TR/16.09	Redundancy: Fans and power supplies: Dual redundant, hot- swappable	
DCH/TR/16.10	Disk Drive Support • Storage subsystem should support 4TB/6TB/8TB or higher NLSAS/SATA/equivalent 7.2K drives in the same device array. • Should be populated minimum 100 TB of storage from day 1 with minimum 20% of storage capacity with SSD drives.	
DCH/TR/16.11	Global Hot Spare • Should have the capability to designate global hot spares that can automatically be used to replace a failed drive anywhere in the system. • Should be configured with required Global Hot-spares for the different type and no. of disks configured, as per the system architecture best practices.	
DCH/TR/16.12	Multipath: Multi-path & Load balancing, MPXIO, IPMP, LACP protocol should be supported.	
DCH/TR/16.13	Capacity: Should be configured with SSD capacity for application storage & NL-SAS drives for video surveillance storage	
DCH/TR/16.14	Thin Provisioning: Array should be supplied with Thin provisioning for the configured capacity.	
DCH/TR/16.15	De- duplication: Array should have capability to provide compression, de-duplication and encryption.	
DCH/TR/16.16	Tiering: Should support inbuilt automated tiering feature that migrates the most frequently accessed data to the SSD/RAM. Necessary licenses for configured capacity if required without additional cost	
DCH/TR/16.17	Snapshots: Should be able to take "snapshots" of the stored data. Offered Storage shall have support to make the snapshot in scheduled or auto snaps. Snapshot should support both block and file.	
DCH/TR/16.18	Replication: Array should have the capability to do remote replication using IP technology	
DCH/TR/16.19	Software Licenses : All the necessary software and licenses to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots, compression, de-dup, replication, auto-tiering for the configured capacity.	
DCH/TR/16.20	Monitoring: Should support the functionality of monitoring of Disk drive and Storage system for all possible hard or soft failure.	
17	**Industrial Ruggedized Switches**	
DCH/TR/17.01	Ports • Should have minimum 8 x of 10/100/1000 RJ45 interfaces with POE+ supporting IEE 802.3af and 802.3at standards and 4 x 1G SFP interface.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should have Simultaneous active 12 or more port 12 with EEE support on all copper port	
DCH/TR/17.02	Performance and Reliability • Should operate at wider temperature range withstands greater shock, vibrations, temperature and EMI/EMC tests. • Should have non-blocking wire-speed architecture. • Should be architected to support real time applications like voice, video, data by having distributed architecture. • Should support IP 30 rating and MTBF value not less than 25 years	
DCH/TR/17.03	Power • Should have DC Redundant power input • Power consumption max 15 W • POE Budget – 240 watts. • Simultaneous 802.3at PoE+ support on all Copper Port	
DCH/TR/17.04	VLAN support (as per industry standard) • Minimum 1024 active VLANS • Dynamic VLAN with VTP / MVRP • IP subnet VLAN • 802.1v • 802.1ad (q-in-q) • Private Vlan	
DCH/TR/17.05	Security • 802.1x support ,MAC-based Authentication • DHCP Server ipv4 & ipv6, Client, Relay, Snooping , option 82/Relay, • ACL based on L2, L3, L4 rules • IP source Guard f. Reverse Power protection and Transient protection -> 15 W peak g. CPU watchdog • Storm Control for unicast, broadcast and multicast. • Cable diagnostics to measure cable length i. Ipv4 & v6 sFlow Agent	
DCH/TR/17.06	Surveillance Traffic data handling support • 8K MAC table • 8 QOS queues per port, DSCP remarking • NTP over IPv6. • Bandwidth control rate limit, Per Vlan port mirror • Ring Protocol for fast failover. Link loss recovery < 50ms • IGMP snooping - v1,v2,v3, MLD snooping , MVR • Minimum 1K Multicast Groups	
DCH/TR/17.07	Management • Should support GUI based software for mass configuration of switches • IP v6 management with support for SSH, Telnet, SNMP, 64k RMON event entries • Support Syslog for alarm • Dedicated Management port with industry standard CLI • PoE management - Scheduling of Power Delivery, Power limit by device type and Power delivery prioritisation • Switch Port Analyzer per vlan • RADIUS (Authentication and Accounting), TACACs+ 3.0 , RMON I and II, DNS Server, Client and Proxy, Configurable LLDP-MED values	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Support for RFC 2544	
DCH/TR/17.08	Industry Certification • CISPR 22,24; ICES-003 Class A;EN 61000-4-2 Electro Static Discharge; EN 61000-4-3 Radiated RF; EN 61000-4-4 Electromagnetic Fast Transients;EN 61000-4-5 Surge; EN 61000-4-6 Conducted RF; EN 61000-4-8 Power Frequency Magnetic Field; EN 61000-4-9 Pulsed Magnetic Field Immunity; RoHS and WEEE compliant; NEMA- TS2	
DCH/TR/17.09	Operating Condition • Temperature and humidity as per city condition and requirement	
DCH/TR/17.10	Accessories • Should be supplied with mounting bracket, DIN rail, power cord, console cable and installation guide with each switch.	
18	**Online UPS-500 VA**	
DCH/TR/18.01	Capacity: Adequate capacity to cover all above IT Components at respective location	
DCH/TR/18.02	Output Waveform: Pure Sine wave	
DCH/TR/18.03	Input Power Factor at Full Load: >0.90	
DCH/TR/18.04	Input: Three Phase3 Wireforover5 KVA	
DCH/TR/18.05	Input Voltage Range: 305-445VACatFullLoad, 50Hz+/-3 Hz	
DCH/TR/18.06	Output Voltage: 400V AC, Three Phase for over 5 KVA UPS	
DCH/TR/18.07	Output Frequency: 50 Hz+/-0.5%(Free running);+/-3%(Sync. Mode)	
DCH/TR/18.08	Inverter efficiency: >90%	
DCH/TR/18.09	Overall AC-AC Efficiency: >85%	
DCH/TR/18.10	UPS Shutdown: UPS should shut down with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Low Battery 4) Inverter over load 5) Over temperature 6) Output short	
DCH/TR/18.11	Battery Back-up: Min 2 Hours and as per design consideration	
DCH/TR/18.12	Battery: VRLA(Valve Regulated Lead Acid), SMF(Sealed Maintenance Free) Battery	
DCH/TR/18.13	Indicators & Metering: Indicators for AC Mains, Load on Battery, Fault, Load Level, Low Battery Warning, Inverter On, UPS on By- pass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.	
DCH/TR/18.14	Audio Alarm: Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.	
DCH/TR/18.15	Cabinet: Rack/Tower type	
19	**Server Load Balancer**	
DCH/TR/19.01	Should be high performance purpose built next generation multi-tenant hardware with multi-core CPU support. Platform should support multiple network functions including application load balancing, application firewall, SSL VPN & global server load balancing functions with dedicated hardware resources for each virtual instance.	
DCH/TR/19.02	Platform should have option to support 3rd party network functions from day one	
DCH/TR/19.03	The appliance should have minimum 8 x10G SFP+ data interfaces from day one	
DCH/TR/19.04	The appliance should support Minimum 64GB RAM and 1*SSL ASICS/FGPA/cards with network virtual function support	
DCH/TR/19.05	Next generation multi-tenant platform should support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each network function should have assigned dedicated hardware resources including I/O interfaces, memory, CPU, SSL card in order to ensure every network functions performs without affecting other functions	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/19.06	The device should support up to 65 Gbps of System throughput	
DCH/TR/19.07	Platform should support multiple network functions in order to cater current and future requirements and performance numbers including throughput, connections, SSL throughput and SSL transactions. Should support upto 16 Network Virtual Functions	
DCH/TR/19.08	The device should have the following features of throughput parameters	
DCH/TR/19.09	Load balancer network function with minimum 15 Gbps of system throughput	
DCH/TR/19.10	Should support up to 4 Million RPS per system	
DCH/TR/19.11	Should support upto 35000 SSL Transactions per second	
DCH/TR/19.12	Should support minimum 20 Gbps of SSL Throughput	
DCH/TR/19.13	Dedicated management interface	
DCH/TR/19.14	Should be able to load balancer both TCP and UDP based applications with layer 2 to layer 4 load balancing support	
DCH/TR/19.15	Should support server load balancing algorithms	
DCH/TR/19.16	Should support for policy nesting at layer4 and layer4, solution should able to combine layer4 and layer4 policies to address the complex application integration.	
DCH/TR/19.17	Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support e-Policies to customize new features in addition to existing feature/functions of load balancer	
DCH/TR/19.18	Traffic load balancing using e-Policies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash IP and SNMP	
DCH/TR/19.19	Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.	
DCH/TR/19.20	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.	
DCH/TR/19.21	Should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers	
DCH/TR/19.22	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	
DCH/TR/19.23	Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.	
DCH/TR/19.24	Proposed solution should support remote access which is 100% client less for web based applications	
DCH/TR/19.25	Should support for CIFS file share and provision to browse, create and delete the directories through web browser	
DCH/TR/19.26	Should maintain original server access control policies while accessing the file resources through VPN	
DCH/TR/19.27	Should support Single Sign-On (SSO) for web based applications and web based file server access	
DCH/TR/19.28	Should have secure access solutions for mobile PDAs, Android, Windows and iOS based smart phones and tablets	
DCH/TR/19.29	Should Support IPV6	
DCH/TR/19.30	Proposed solution should provide machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. MAC address to provide secure access to corporate resources.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/19.31	Should support following Authentication methods: - LDAP, Active directory, Radius, secureID, local database, and certificate based authentication and anonymous access.	
DCH/TR/19.32	Should provide comprehensive and reliable support for high availability both at device level and Virtual function level	
DCH/TR/19.33	Device level HA should support synchronization of network functions configuration from primary/master device to secondary/slave device	
DCH/TR/19.34	ADC virtual function should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization, system memory, process health check and gateway health check to support the failover in complex application environment	
DCH/TR/19.35	ADC VF Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway	
DCH/TR/19.36	13. ADC VF Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.	
DCH/TR/19.37	The appliance should have SSH CLI, Direct Console, SNMP, and Single Console per Cluster with inbuilt reporting.	
DCH/TR/19.38	The appliance should provide detailed logs and graphs for real time and time based statistics	
DCH/TR/19.39	Should capture, log and display traffic related data to analyze for security incidents.	
DCH/TR/19.40	Should support XML-RPC for integration with 3rd party management and monitoring of the devices.	
DCH/TR/19.41	The appliance should have extensive report and logging with inbuilt tcp dump like tool and log collecting functionality	
DCH/TR/19.42	Should be able to send security incidents via SYSLOG	
20	**Centralized AV and Anti-Spam**	
DCH/TR/20.01	Single Agent: Should be only single agent that combines all the critical components for total security on the endpoint. (Antivirus, Antimalware, Firewall, VPN Client, Virtual Browser etc.)	
DCH/TR/20.02	Personal Firewall: Firewall should block unwanted traffic, prevents malware from infecting endpoint systems, and makes them invisible to hackers.	
DCH/TR/20.03	Program Control with Program Advisor: Program Control ensures that only legitimate and approved programs are allowed to run on the endpoint. Program Advisor is a real-time Vendor knowledge base of over a million trustworthy applications and suspected malware used to automatically set the Program Control configuration.	
DCH/TR/20.04	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses	
DCH/TR/20.05	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses	
DCH/TR/20.06	Deep scan: Should Scan Runs a detailed scan of every file on selected scan targets	
DCH/TR/20.07	Scan target drives: Should Specifies directories and file types to scan	
DCH/TR/20.08	Scan exclusions: Should Specify directories and file extensions not to be scanned	
DCH/TR/20.09	Treatment options: Should Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete	
DCH/TR/20.10	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware	
DCH/TR/20.11	Full-system scan: Should Scans local file folders and specific file types	
DCH/TR/20.12	Deep-inspection scan: Should Scan every byte of data on the computer	
DCH/TR/20.13	Scan target drives: Should Specify which directories and file types to scan	
DCH/TR/20.14	Scan exclusions: should Specify directories and file extensions not to be scanned	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/20.15	Treatment options: Should Enable choice of action agents should take upon detection of virus: Automatic, notify, or confirm	
DCH/TR/20.16	Browser Security: • Should Support latest versions leading web browsers i.e. IE, Mozilla, Chrome, Safari etc. • Should Provide a dual browser mode that segregates corporate data from the Internet • Should Allow users the freedom to surf with full protection against malicious software that is automatically downloaded and phishing attempts • Should Secure through unique browser virtualization, heuristic anti-phishing and malware site detection • Should Support Browser Virtualization • Should Support Signature & Heuristic Phishing Protection • Should Support Site Status Check • Should Support Centralized Browser Security Policy Management • Should Support Centralized Browser Security Event Logging & Reporting	
DCH/TR/20.17	Management Platform Support: • Operating systems: Should Support Windows Server 2008, 2012, 2016 • Browsers: Should Support Internet latest version of leading web browsers • Client Platform Support • Should support Windows 8, 10 (32 & 64 bit), Linux	
DCH/TR/20.18	Gateway Security: • Should provide fast protection at the gateway across multiple protocols for inbound and outbound web traffic • The solution should provide protection against malware threats on all Web 2.0 file transfer channels • The solution should offer in built URL filtering with flexible policy controls, and in- depth reporting and alerts (the URL filtering license is required) • Virus Gateway should have option to configure to respond to virus detection in several ways i.e. Delete the file, quarantine the file, Alert email • The solution should have advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications • In terms of SMTP anti-spam scanning the solution should be capable of acting as mail relay or MTA by itself. • Should have facility to block files based on file extensions over HTTP, FTP, SMTP, POP3 as well as IMAP • The solution should be able to detect compromised endpoints by network fingerprinting and behavioral modeling and should be able to block these infected end points by resetting the connection attempts to their phone home sites • System should classify traffic into protocols without relying on specific port numbers (for example, port 80 for HTTP) • The solution should support load balancing for scanning, so that the traffic which needs to be scanned can be load balanced across the boxes in the cluster • Comprehensive Web reporting and alerting should be available out of box and should offer following reports:- - Most accessed Web sites - Most active users - Spyware-infected computers	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	- Most common malware • Reports should be available by IP address or user if active directory integration is done	
DCH/TR/20.19	Web Content Filtering: • Should be an integrated solution within the firewall or a standalone hardware appliance. • Web content filtering solution should work independently without the need to integrate with proxy server • Web based management through https and command line interface support • Should have facility to block URL' based on categories • The solution proposed should support at least 45+ million URLs categorized into 60+ default website categories across 50 different languages and 100+ protocol applications. • URL Database should be updated regularly • Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key logger • Should have configurable parameters to block/allow unrated sites • Should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable • Should have options to customize the block message information send to end users • Should have facility to schedule the configurations so that non-work related sites are blocked during office hrs and allow access to all sites except non harmful sites during non-office hrs. • Should have facility to configurable policy options to block web sites based on content • The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories • Should have configurable policy options to define the URLs what needs to be blocked • Should have configurable policy options to define the URL exempt list • The solution should be able to block spywares/adwares etc. • The solution should have options to block java applets, active X as well as cookies • The solution should have options to configure in such a way that in case if the primary fails the secondary becomes active without manual intervention • The solution should have options to block download of files over internet based on file extension (e.g. *.avi, *.mpeg, *.mp3 etc.)	
DCH/TR/20.20	URL Filtering Features: • The solution should provide security related website categories to address specific security concerns include, but not limit to : - Malicious Websites - Key Loggers - Phishing and other online frauds - Spyware – including drive-by spyware download and back channel communication by spyware installed on local client. - Potentially Unwanted software - Bot Network - The solution proposed should have capabilities to block back channel	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	communication from spyware / key-logger infected machines to hacker host sites - The solution should have the ability to apply different policies to different users, different client IP address and address range and different user groups - The solution should have the capability for Embedded URLs in selected search engines can also be filtered individually - The solution should support Time based Quota policies for URL categories, users, IP, networks, user groups etc. - The solution should have the ability for users to define —Regular Expressions‖ to precisely identify targeted URL - Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key loggers - The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories - The solution should support risk classes for Security, Legal Liability, Productivity Loss, Bandwidth Loss and Business Usage at least so that predefined URL categories can be associated with these risk classes - Ability to collect certain uncategorized or security related URLs to feedback, improve URL categorization and security effectiveness - The solution should support display of web based block pages and the block pages should be customizable	
DCH/TR/20.21	Spam Filtering: • The proposed solution should Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading technologies and response capabilities, leverage adaptive reputation management techniques that combine global and local sender reputation analysis to reduce email infrastructure costs by dropping up to 90% of spam at the connection level, Filter email to remove unwanted content, demonstrate regulatory compliance, and protect against intellectual property and data loss over email, Secure and protect other protocols, such as public IM communications, using the same management console as email, Obtain visibility into messaging trends and events with minimal administrative burden. • The proposed solution should automatically back up all configuration and quarantine databases on the appliance at specified intervals. Administrators should be given an option to store data on the local machine or a remote server. • Should be able to detect spam mails in SMTP, POP3 as well as IMAP protocols • The proposed solution should have inspection facility on the header and body of the mail to check for spam URI content and identify whether the mail is a spam mail or not • Option should be available to manually configure multiple RBL& ORDBL servers to check for spam mail • Should have options to configure white list as well black list based on IP address and validate against the same to detect whether a mail is spam mail or not • Should have configurable parameter to enable HELO DNS lookup to check	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	whether a mail is a spam or not. • Should have configurable parameter to enable return email DNS lookup to check whether a mail is a spam or not. • Should have provision to define banned key words and check against that key words to identify spam mails. • Should have options to define mime headers and check against the same to identify spam mail. • The solution should have Global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections. • Solution should be scalable to incorporate the following with no installation of component on clients should need be in future: - Email archiving, mail box archiving, file archiving, personal folders (.pst files) consolidation, journaling, discovering mails - Integration with data loss prevention technologies to check loss of data through mails at gateway - The proposed solution should have an option to restore an appliance to its original image configuration. - Should have configurable spam actions for detected spam mails (e.g. tag the mail, delete the spam mail etc.).	
DCH/TR/20.22	Ability to scan through all file types and various compression formats. Ability to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls.	
DCH/TR/20.23	Should update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)	
DCH/TR/20.24	Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
DCH/TR/20.25	Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.	
DCH/TR/20.26	The solution should provide protection to multiple remote clients	
DCH/TR/20.27	Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification	
DCH/TR/20.28	Should be capable of providing multiple layers of defense	
DCH/TR/20.29	Shall have facility to clean, delete and quarantine the virus affected files.	
DCH/TR/20.30	Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.	
DCH/TR/20.31	Should support in-memory scanning so as to minimize Disk IO	
DCH/TR/20.32	Should support Multi-threaded scanning	
DCH/TR/20.33	Should support scanning of nested compressed files	
DCH/TR/20.34	Should support heuristic scanning to allow rule-based detection of unknown viruses	
DCH/TR/20.35	All binaries from the vendor that are downloaded and distributed should be signed and the signature verified during runtime for enhanced security.	
DCH/TR/20.36	Ability to scan through all file types and various compression formats. Ability to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls.	
DCH/TR/20.37	Should update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)	
DCH/TR/20.38	Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
DCH/TR/20.39	Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/20.40	The solution should provide protection to multiple remote clients	
DCH/TR/20.41	Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.	
DCH/TR/20.42	Should be capable of providing multiple layers of defense	
DCH/TR/20.43	Shall have facility to clean, delete and quarantine the virus affected files.	
DCH/TR/20.44	Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.	
DCH/TR/20.45	Should support in-memory scanning so as to minimize Disk IO.	
DCH/TR/20.46	Should support Multi-threaded scanning	
DCH/TR/20.47	Should support scanning of nested compressed files	
DCH/TR/20.48	Should support heuristic scanning to allow rule-based detection of unknown viruses	
21	**Mail & Messaging Solution**	
DCH/TR/21.01	General: • Network/Server edition should run on Linux /Windows • Desktop client should run on Mac, Linux and Windows • Solution should be based on open standards • Should support advanced search and file indexing for large inboxes • Ability to use custom logos in the web interface • Should support e-mail, Address Book, Calendar, Task & File Server • Should support real-time backup and restore • Should support clustering/High-Availability • Ability to access the Mail server via IMAP clients, with the option to connect over SSL/TLS • Ability to access the Mail server via POP clients, with the option to connect via SSL/TLS • Comprehensive suite of standards-based web services APIs enabling seamless integration with other applications • Ability to utilize Active Directory for user authentication and/or Global Address List • Admin can configure an initial password in the migration wizard and import wizard for newly provisioned accounts • Should support multi-tenancy • Should support e-mail Archiving & Discovery • Should have rich, interactive, web-based interface for end user functions (access via HTTP or HTTPS) • Ability to customize the colors and appearance of the web interface • Option to check and correct spelling in a mail message, calendar appointment, or web Document • Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access) • Ability to share Address Books, Calendars, and Notebooks (Documents) with external users via a custom password (read access) • Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user-defined names and colors • Option to quickly view attachments in HTML format • Should support conversations span folders • Ability to create personal folders and folder hierarchies • Ability to print a message and see a print preview • Ability to sort messages based on subject, date, or sender	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Ability to flag/unflag messages/conversations for follow up • Ability to define filter rules and priorities for incoming messages • Ability to enable/disable a custom away message • Ability to add a custom signature to a message • Option to popup a separate window when composing a message • Ability to save in-progress messages to a Drafts folder • Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox • Option to Reply or Reply-All while retaining the attachments from the original message • Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete) • Right-clicking an email address displays a menu of actions to take on that address (e.g. view website, add/edit contact, create filter, search for messages) • Ability to export a set of messages as a ZIP file • Ability to toggle between Reply and Reply-All while composing a reply • Users can set their default preference for viewing messages in the reading pane • Users can set the default font family, font size and font color to use when composing email messages and Documents pages • Users can share their mailbox folders and set the permission levels to manage or to view-only • Users can insert inline images in email messages and calendar appointments • Admin can configure the maximum number of characters used in a signature	
DCH/TR/21.02	Address Book: • Business card view of Contacts • List view of Contacts with preview pane • Ability to import/export Contacts in .csv format • Ability to import/export contacts in vCard (.vcf) format • Ability to print a single Contact or list of Contacts and see a print preview • Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages) • Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact • Ability to create multiple Address Books in a single mailbox • Ability to move/copy contacts from one Address Book to another (based on access privileges) • Ability to create group contact lists in their user Address Books • Address book displays individual contact information in tabbed view • Photos and images can be uploaded to contacts in Address Books	
DCH/TR/21.03	Calendar: • Ability to schedule personal appointments • Ability to schedule meetings and view attendees' free/busy information • Ability to book resources (locations, equipment, etc.) for a meeting • Ability to configure a resource to auto-respond to scheduling requests based on availability • Option to enable an alert popup for upcoming appointments • Appointments/schedules are automatically displayed in the users current time zone	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Ability to set an explicit time zone for an appointment • Ability to view calendars in Day, Week, Work Week, or Month views • User setting for the first day of the week; value chosen impacts the Week calendar view • Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views • Ability to quickly mark Accept/Tentative/Decline from calendar views • Ability to print calendars in day, week, work week, or month views and see a print preview • Hovering over an appointment in calendar view displays additional appointment details • Option to display a miniature calendar at all times • Hovering over a date in the mini-cal displays calendar information for that date • Right-clicking on the mini-cal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages) • Ability for a user to create multiple calendars within a single account • Ability for a user to designate which calendars will be included in the user's free/busy calculations • Ability to subscribe to an external calendar in i-Calendar (.ics) format • Ability to publish/export a calendar in i-Calendar (.ics) format • Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color • When viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot • Users can import calendar i-Calendars (.ics) • Administrators can configure the Calendar feature to be able to create only personal appointments • Users can search for appointments within their calendars • Public calendars display in HTML read-only format	
DCH/TR/21.04	Tasks: • Add tasks and set the start and due date, set the priority and keep track of the progress and percentage complete • Share task lists with internal and external users and set permission levels to manage or to view-only • Users can organize task lists into folders • Users can sort tasks by Status or Due Date • Users can set the priority of tasks to high, normal or low • Individual tasks can be tagged • Files can be attached to a tasks	
DCH/TR/21.05	Documents: • Ability to create rich web Documents with WYSIWYG or HTML editing • Ability to create a notebooks as a Document repository and as a mechanism for navigating through Documents • Ability to create multiple notebooks in a single mailbox • Ability to create a notebook that is shared by everyone within a domain • Ability to insert links in Documents to other Documents or to external URLs • Ability to upload Attachments as Documents • Ability to embed rich content objects as independently editable items inside a web	
DCH/TR/21.06	Search:	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Server-side indexing of mailbox content, enabling fast and efficient search from the web interface • Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.) • Ability to use text commands to execute searches • Advanced interface for building searches • Ability to search for a specific item type (Mail, Contacts, Documents, etc.) or across item types • Ability to search using a prefix plus a wildcard • When using Search Builder, the search result set updates continuously as search conditions are changed • Ability to save searches for subsequent one-click re-execution • Ability to search for items that contain specific keywords • Ability to search for items with a specific date or within a specific date range • Ability to search for items that contain an attachment • Ability to search for items that contain an attachment of a certain type(s) • Ability to search for items that have a specific flagged/un-flagged status • Ability to search for items that are in a specific folder • Ability to search for items based on storage size • Ability to search for items based on read/unread status • Ability to search for items with specific recipients in the To /Cc fields • Ability to search for items from a specific sender • Ability to search for items based on subject • Ability to search for items that include a specific Tag(s) • Ability to search for items that were sent to or received from a specific domain • Ability to search for Contacts in a Shared Address Book • Ability to search for content inside attachments • Can search for appointments in calendars up (up to 180 days) • Administrator can disable the indexing of junk mail	
DCH/TR/21.07	Domain-level Management: • Ability to create and manage multiple mail domains within a single instance of Messaging Solution • Ability to use different Global Address Lists for each domain • Ability to use different authentication stores for each domain • Ability to delegated domain-level administrators to manage users and other settings specific to a domain	
DCH/TR/21.08	Storage: • Messages (including attachments) sent to multiple users are stored once to optimize storage space • Ability to set quotas for mailbox size and number of Contacts • View of mailboxes sortable by quota, total mailbox size, or % quota consumed • Ability to define retention policies for all messages, trashed messages, and/or junk messages • Ability to move a mailbox(es) from one server to another without requiring system downtime or affecting other mailboxes • Ability to run a regularly scheduled process that moves older messages to a secondary storage volume	
DCH/TR/21.09	System and Health Security: • Should have native anti-virus & anti-spam mechanism	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Administrator interface setting to specify spam quarantine and kill thresholds • Messages that users mark as Junk / Not Junk are automatically fed into the spam training engine • Administrator interface setting to define the update frequency for virus signatures • Ability to enforce client authentication to the SMTP server before relaying mail (with option to require authentication over TLS) • Graphical display of system activity including disk usage, message volume, and AS/AV results • Ability to monitor the status of all core system servers/services in a single view • Ability to block attachments based on criteria such as attachment type or size • Ability to enforce that attachments be viewed as HTML, enabling risk-free attachment viewing without requiring attachment-native applications on the viewer's machine • Install and manage certificates from the administration console	
DCH/TR/21.10	Compatibility and interoperability: • MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server • Online/offline status is automatically detected, enabling the user to work without having to specify their connection status • Synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Outlook performance	
DCH/TR/21.11	Mobile Devices: • AJAX Mobile Web Browser • i-Phone Email, Contact, Calendar sync • Windows Mobile and other smartphone Email • Email, Contact, Calendar sync	
22	**Identity Access Management**	
DCH/TR/22.01	Solution should provide the ability to make real-time course-grained authorization decisions such as a whether to grant access to an application.	
DCH/TR/22.02	Solution should provide the configurable ability to restrict or allow concurrent logins by the same user	
DCH/TR/22.03	Solution should deny assignment of one role to a user, based on their existing role assignment (mutually exclusive roles).	
DCH/TR/22.04	Solution should support disablement/deletion of unused or expired accounts	
DCH/TR/22.05	Solution should provide a clear audit log of “impersonation” events to enable investigation of who has performed the functions or changed data using an external user’s account	
DCH/TR/22.06	Solution should be able to connect to various applications with independent databases so as to include all user profiles from those applications.	
DCH/TR/22.07	Solution should perform basic audit and logging capabilities.	
DCH/TR/22.08	Solution should aid in documenting clearly all systems access in a global repository, to make it easier to terminate access in the future	
DCH/TR/22.09	Solution should support existing IT Compliance reporting for User Access Verification by periodically auditing the account setup on each system, to measure compliance with standards.	
DCH/TR/22.10	Solution shall enforce strong password management features	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
23	**Enterprise Database**	
DCH/TR/23.01	Database License should beun-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.	
DCH/TR/23.02	Databases shall support multi-hardware platform.	
DCH/TR/23.03	RDBMS should support relevant Unicode with Indian Language support	
DCH/TR/23.04	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), raster data as well as the metadata.	
DCH/TR/23.05	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.	
DCH/TR/23.06	Database shall have built-in backup and recovery tool, which can support the online backup.	
DCH/TR/23.07	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.	
DCH/TR/23.08	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.	
DCH/TR/23.09	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single /multiple database.	
DCH/TR/23.10	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.	
DCH/TR/23.11	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases	
DCH/TR/23.12	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real time or near real-time reports from the DR site without stopping the recovery mechanism.	
DCH/TR/23.13	Ability to recover the node on fly or with limited timelines with-out Unloading/ reloading data.	
DCH/TR/23.14	RDBMS should provide continuous availability features to address hardware failures, instance failures, human errors like accidental deletion of data, tables etc.	
DCH/TR/23.15	Database shall provide native functionality to store and retrieve XML, Images and Text data types.	
DCH/TR/23.16	Database shall provide native functionality to store XML, within the database and support search, query functionalities.	
DCH/TR/23.17	RDBMS should support spatial data types.	
DCH/TR/23.18	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.	
DCH/TR/23.19	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical	
DCH/TR/23.20	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.	
DCH/TR/23.21	Database shall be having native auditing capabilities for the database.	
DCH/TR/23.22	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.	
DCH/TR/23.23	Availability of recovery/restart facilities of the DBMS.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/23.24	Automated recovery/restart features provided that do not require programmer involvement or system reruns.	
DCH/TR/23.25	Program restart should be provided from the point of failure.	
DCH/TR/23.26	RDMS should have the ability to manage recovery/restart facilities to reduce system overhead.	
DCH/TR/23.27	Provides extra utilities to back up the databases by faster means than record by record retrieval.	
DCH/TR/23.28	The database should provide controls over who, when, where and how applications, data and databases can be accessed.	
DCH/TR/23.29	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.	
DCH/TR/23.30	The database should provide multi-factor authentication based controls and policies preferably taking account of application context etc.	
DCH/TR/23.31	Should provide adequate auditing trail facility. Audit trail should also be maintained at database level for any changes made in database and it should be ensured that these audit trails cannot be manipulated by anyone including super users and DBAs.	
DCH/TR/23.32	System should record the date and time stamp for all records generation/ modification	
DCH/TR/23.33	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting	
24	**Directory Services**	
DCH/TR/24.01	Should be compliant with LDAP v3	
DCH/TR/24.02	Support for integrated LDAP compliant directory services to record information for users and system resources	
DCH/TR/24.03	Should provide authentication mechanism across different client devices / PCs	
DCH/TR/24.04	Should provide support for Group policies and software restriction policies	
DCH/TR/24.05	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.	
DCH/TR/24.06	Should provide support for X.500 naming standards	
DCH/TR/24.07	Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user	
DCH/TR/24.08	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user	
DCH/TR/24.09	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user	
DCH/TR/24.10	Should support directory services integrated DNS zones for ease of management and administration /replication.	
25	**DDOS (Distributed Denial of Service)**	
DCH/TR/25.01	Hardware & Performance • Secure application delivery functionalities should be offered from a single OEM. • Should provide integrated functionalities of Link Load Balancing, SSL and DDoS Protection. • Should have Min 8 x 10G ports and 4 x 40GE QSFP+ ports • Should provide minimum throughput of 60 Gbps • Should support minimum SSL TPS of 80k (RSA 2k keys) and minimum 48K (with ECDSA 256 key). • Should support minimum 30 Gbps hardware based Compression throughput • Should support minimum 35 Gbps of SSL throughput	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should provide HW based SYN cookies Protection • Should support minimum 2M DNS Query Per Second • Should support minimum 100 Million L4 connection	
DCH/TR/25.02	Availability Features • Should offer out of band programming for control plane along with data plane scripting for functional like content inspection and traffic management • Should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover • Should support global server load balancing between DC and on premise/cloud based DR. The proposed solution should support Link Load Balancing functionality. • Should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	
DCH/TR/25.03	Security Functionalities • Should provide comprehensive security both at network and application level via Layer 4 to Layer 7 DDoS and SSL on a single device. • Detects and prevents zero-day DNS-flood attacks. ▪ DNS query limit ▪ DNS Nxdmain attack protection ▪ DNS TCP active authentication mechanism • Should support integration with proposed WAF solution. • Should be able to take threat intelligence feed to reveal inbound communication with malicious IP addresses, and enable granular threat reporting and automated blocking. • Should provide protection against SYN Flood, DoS/DDoS attack (including VOIP/SIP based DDoS), DNS based attack, Zero-day attacks • Should be stable and not affect service availability even upon any system fault • Should have functionality to signal to Cloud Scrubbing center • Should detect any DDoS traffic and mitigate any DDoS attack without interrupt legitimate traffic and customer services. • Detection and Mitigation of volumetric DDOS traffic should occur within 3 min. • Should support SSL offloading using both RSA and ECC based keys • Should perform comprehensive countermeasure to protect against zero day attack, Challenge – Response Mechanism, which should be able to detect and protect attacks in real time through inbuilt Captcha Mechanism • Geolocation IP address database to identify the source of the attack origin and IP Reputation Mechanism to identify the Blacklisted TOR Networks or Proxy IP address to Block the request immediately. • Protection from DNS based attacks originated from Botnets of connected IOT devices like sensors like CCTV cameras, parking sensors, thermostat etc.	
DCH/TR/25.04	Management, Reporting and Other • Proposed solution should be manageable from the same management platform which manages WAF and DDoS. • Should Support integration with SIEM and other Monitoring and Reporting solution	
26	**SIEM (Security Information and Event Management)**	
DCH/TR/26.01	• Should encompass log, packet and end point data with added context and threat Intelligence.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Should provide complete network visibility through deep packet inspection high-speed packet capture and analysis.	
DCH/TR/26.02	SIEM for Logs and deep packet inspection should be from same OEM.	
DCH/TR/26.03	Should be a physical appliance form factor with following components: • Management & Reporting • Normalization and Indexing • Correlation Engine • Data Management	
DCH/TR/26.04	Should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.	
DCH/TR/26.05	Should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP, and Encryption.	
DCH/TR/26.06	Should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.	
DCH/TR/26.07	• Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. • In addition solution should provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP/Device etc.	
DCH/TR/26.08	Should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.	
DCH/TR/26.09	Should support minimum 30,000 EPS and packet appliance should support upto 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.	
DCH/TR/26.10	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 100,000 EPS.	
DCH/TR/26.11	• Should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. • Should be sized to provide online storage for 1 year at central site. Both raw logs and normalized logs should be made available with minimum 90 TB of storage provided by OEM	
DCH/TR/26.12	Should incorporate and correlate information that enables the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.	
DCH/TR/26.13	Should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required	
DCH/TR/26.14	Should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.	
DCH/TR/26.15	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration	
DCH/TR/26.16	Should store RAW packet DATA for 7 days and normalized packet data for 30 days for forensics.	
DCH/TR/26.17	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.	
DCH/TR/26.18	Should be able to filter the captured packets based on layer-2 to layer-7 header information.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/26.19	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.	
DCH/TR/26.20	Solution should be able to provide the complete platform to perform Network forensics solution	
DCH/TR/26.21	Solution should be able to detect malicious payload in network traffic • Detect and reconstruct files back to its original type • Detect hidden or embedded files • Detect and flag out renamed files	
DCH/TR/26.22	The solution should have the ability to capture network traffic and import PCAP files using the same infrastructure.	
DCH/TR/26.23	• Should encompass log, packet and end point data with added context and threat Intelligence. • Should provide complete network visibility through deep packet inspection high-speed packet capture and analysis.	
DCH/TR/26.24	SIEM for Logs and deep packet inspection should be from same OEM.	
DCH/TR/26.25	Should be a physical appliance form factor with following components: • Management & Reporting • Normalization and Indexing • Correlation Engine • Data Management	
27	**Secure Email Gateway**	
DCH/TR/27.01	Should be an dedicated appliance based solution or Virtual Application image for email security	
DCH/TR/27.02	• Should have feature of virus scanning engine strip the infected attachments • Should detect known or suspect secure-risk URLs embedded in the email, which are reliable indicators of spyware, malware or phishing attacks.	
DCH/TR/27.03	Should have performance capability of processing more than 2, 00,000 messages per hour.	
DCH/TR/27.04	• Should have close to 100% virus detection rate for known viruses. Should have multiple AV engines for anti-virus and malware scanning. • Should provide proactive virus detection methods for new email-borne virus. • Should have feature of virus scanning engine strip the infected attachments.	
DCH/TR/27.05	• Virus engine should support scanning by inbound, outbound and internal direction and configure the policy per direction. • The Solution should have the access and manipulate the quarantined virus emails.	
DCH/TR/27.06	• Should provide an attachment scanning capability to detect file-based spam messages. • Should also allow users to report SPAM mails.	
DCH/TR/27.07	• Should support URL classification of the embedded links and it contributes for SPAM detection. • Should support image based spam detection capability, such as the pornography images within the email and it allow customer to adjust the sensitivity level.	
DCH/TR/27.08	• Should support dictionaries scanning and dictionaries are built-in the product and allow customer to create his own dictionary. • Should have at least 1500+ predefined content rules inbuilt with Email Security & embedded in the product	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/27.09	• Should report the false positive email and a button in the quarantine queue thus customer can simply click to have a report	
DCH/TR/27.10	• Should be able to look for content in the email header, body of message and also attachments	
DCH/TR/27.11	• Should be able to restrict incoming, outgoing and internal mails based on file types, file size and also by file name and also through a combination of them.	
DCH/TR/27.12	• Should be able to fingerprint files, folders, databases and prevent the information from being sent over outbound mails. • Should have pre-defined dictionaries, key phrases to detect financial terms, offensive language etc.	
DCH/TR/27.13	• Should have capabilities to quarantine mails with content that violates the policy and notify sender or sender's manager automatically. The mails that are quarantined because of content control policies should be released if the sender's manager replies to the notification mail	
DCH/TR/27.14	• Should perform image based filtering. • Should use sophisticated analytical algorithm to analyze image to determine attributes that indicate the image may be of a pornographic or non-pornographic nature in known and unknown spams emails.	
DCH/TR/27.15	• Should have capability to analyze text inside image going through email. • Should monitor and control sensitive email download to mobile devices through active sync	
DCH/TR/27.16	• Should allow setting SMTP greeting message, delay time and the full qualified domain name for SMTP session establishment.	
DCH/TR/27.17	• Should provide the capability of connection control and message rates control for inbound and outbound respectively. • Should support policy based TLS encryption between mail domains.	
DCH/TR/27.18	• Should have directory harvesting and DoS prevention capabilities. • Should support internal sender authentication.	
DCH/TR/27.19	• Should provide real time IP reputation system. • Should allow the administrator to specify the re-try time for a delivery failure.	
DCH/TR/27.20	• Should support IP/address/domain based whitelist and blacklist. • Should support user group (LDAP) or domain based routing and delivery.	
DCH/TR/27.21	• Should support message stamping by adding notes or disclaimer in the message.	
DCH/TR/27.22	• Should have capability for Outbound throttling by IP/address.	
DCH/TR/27.23	• Should support Inbound mail routing delivery preferences to accommodate larger, more complex network	
DCH/TR/27.24	• Should support centralized management, including policy configuration, quarantines and logs/reporting. • Should support the real-time graphical and chart-based dashboard for the summary of email filtering activities.	
DCH/TR/27.25	• Should support quarantine administrator role. Thus only the delegated administrator is allowed to access the message in specific queue.	
DCH/TR/27.26	• Should search a message in the queue and should have multiple options.	
DCH/TR/27.27	• Should have option for end user notification for email quarantining letter to be customized and click boxes that enable the user to release e-mail, report false positives, add senders to allow-or block lists and direct links to personal email management portal.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/27.28	• Should allow where Administrator can specify which queues can be accessed by end user	
DCH/TR/27.29	• The Personal management portal should be a web-based UI for end users. Should allow email reply to release the email quarantined by solution.	
DCH/TR/27.30	• Should support native system backup and software update functionality.	
DCH/TR/27.31	• Should pre-built report templates which the administrator can use for generating reports. • Should support real time graphical and chart based dashboard for the summary of email filtering activities.	
DCH/TR/27.32	• Should support custom report creation in HTML, Excel and PDF.	
DCH/TR/27.33	• Should be able to consolidate reports from multiple boxes for centralized logging and reporting. • Should have capabilities to automatically deliver reports based on schedule to selected recipients	
DCH/TR/27.34	• Should provide detailed information on messages to comprehensively track messages. • Should allow parameters to be defined for searching message logs.	
DCH/TR/27.35	• Should have True Source IP Detection and Connection Blocking feature should work even if Email Security is deployed behind Corporate Email Relay Server/Firewall SMTP	
DCH/TR/27.36	• Should have option to monitor traffic in real time for easier troubleshooting. • Should have a central end user management portal for multiple appliances.	
DCH/TR/27.37	• Should allow end users to release mails from quarantine if approved. • Should provide capabilities for end users to search on quarantined messages specific to them.	
DCH/TR/27.38	• Automatic notifications should be sent to end users whenever mails are quarantined for them. The notification message to end users should be completely customizable.	
DCH/TR/27.39	• Should allow end users to create their own personal allow and block lists. • Should allow administrators to define which queues can be accessed by end user	
DCH/TR/27.40	• Should able to provide the complete forensics of the sensitive outbound data based on the policy defined and should be able to quarantine and release as per automated workflow	
DCH/TR/27.41	• OEM should have its own support center in India	
28	**Application Encryption Solution**	
DCH/TR/28.01	Application level encryption • Centralize control of application-layer encryption and file system encryption • Secure sensitive data across a broad range of platforms and on-premises and PaaS environments • Stop malicious DBAs, cloud administrators, hackers and authorities with subpoenas from accessing valuable data • Streamline large-scale encryption migrations with Batch Data Transformation utility • Required encryption of specific data or database fields at the application, before data is stored encrypts data as either NIST approved AES-CBC or Format Preserving Encryption (FPE)	
DCH/TR/28.02	Supported environments: Microsoft .NET 2.0 and higher, Java 7 and 8, C	
DCH/TR/28.03	Integration standard: OASIS PKCS#11 APIs	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
DCH/TR/28.04	Encryption: AES, Format-preserving encryption FF3	
DCH/TR/28.05	Performance: 400,000 credit card size encryption transactions per second (e.g. single thread, 32 core, 16GB, C)	
DCH/TR/28.06	Policy and key administration: Centralised Security Manager	
DCH/TR/28.07	Character support: ASCII, Unicode	
DCH/TR/28.08	Data Access Audit and Report • should provide fine-grained auditing records that show system accounts and processes accessing data based on security policy • should support integration with SIEM other solution include and deliver centralized access audit and monitoring report	
DCH/TR/28.09	Certification & Validations • The encryption key manager should be Common Criteria (ESM PP PM V2.1) certified • The encryption key manager should have option with FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level Certified	
DCH/TR/28.10	High Performance Data protection solution should support hardware cryptographic acceleration including • Intel and AMD AES-NI • SPARC encryption • IBM P8 cryptographic coprocessor	
DCH/TR/28.11	• Key Management • The proposed solution should be able to manage Keys (KMIP compliant) for third party applications	
DCH/TR/28.12	File level Encryption Should be able to support file level encryption in transparent manner. No downtime is expected while data is transformed into encrypted data.	
29	**Data Encryption**	
DCH/TR/29.01	Separation of Duty and Privileged User Access Control • The solution should be able to protect data-at-rest against root/system privileged user account access. It should also protect file level encryption. • Proposed data protection solution should support fine-grained policy to enable administrator to perform activity like file archive and backup, without access to the data content itself. • The proposed solution should support a separation of duties (SoD) to meet rigorous compliance rules including PCI DSS, HIPAA/HITECH and government data breach policy. The vendor should provide compliance whitepaper to prove such support capability • Proposed solution should support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log. Should have a seamless SIEM Integration. • Should protect the unstructured data (file-shares, files and folders) including big data.	
DCH/TR/29.02	Support Transparent Data Encryption • The proposed data protection and encryption solution should support transparent data protection on all major operating system including: - Microsoft: Windows Server, 2008, 2012 - Linux: Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server, Oracle RedHat Compatible Kernel and Ubuntu - UNIX: IBM AIX, HP-UX, and Solaris Database	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• There should not be any changes in the storage space after the encryption. • Proposed data protection solution should be able to secure both structure database information and unstructured files such as PDF, spreadsheet, scripts, images, audio/video recordings and extract-transformation-load batch files • Proposed data security solution should have minimum performance impact to database transactions with not more than 10% performance overhead on transactions. MSI should provide benchmark report to prove the performance claim • The data transformation should not involve any downtime and live transformation is expected to achieve high Performance Encryption with 100% System Uptime. • Solution should be able to enforces access controls based on – “resources”, “processes”, and “time based access” so that only the defined resources can be accessed with the defined processes and defined users/groups at any given time - Ability to learn the effect of policies (learn mode) before actual encryption is applied is must. - not only appliance but agent also needs to be FIPS certified	
DCH/TR/29.03	Application Encryption and Tokenization • The data protection solution should support format preserving tokenization • The proposed tokenization and masking solution should provide REST API • The data masking solution should support - dynamic masking through policy based masks - Teradata V14 and V14.1 database encryption with UDF - vaultless tokenization - vault based tokenization - gateway to encrypt data stored on S3 and Box	
DCH/TR/31.04	Key Management and KMIP • Should be able to support KMIP client • Should be certified to support Nutanix KMIP • Should provide centralized key management for Oracle and MSSQL TDE master key. • Should support 2-factor authentication with RSA. • Should provide centralized audit for security administration access, key creation, policy changes, data access log and so on. • Should provide application encryption support with Java, C/C++, and .Net API. • Should support LDAP and Microsoft /Linux Active Directory authentication • Should support industry proven cryptograph security standard:3DES, AES128, AES256, ARIA128, and ARIA256 • and asymmetric key RSA-4096/2048, SHA-256 algorithm • The Key management repository should provide virtualization option, with OVF image for deployment option • Hardened Operating System, root account should be disabled, all unnecessary software packages should be removed. A firewall in place that only opens a limited set of required ports.	
DCH/TR/29.05	Installation and Deployment • Proposed data security and encryption solution should support transparent deployment which does not require application code change.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• The proposed data protection solution should support cloud deployment with Amazon AWS, Rackspace • The proposed data protection solution should support deployments including physical, virtual and cloud based servers with minimal administrative overhead. • The proposed data protection solution should support a centralized policy and key management, with highly configurable security and policy enforcement provide granular access control and audit. • The proposed security repository should support high-availability clustering configuration across Local Area Network (LAN) and across geographies over Wide Area Network (WAN). Vendor should provide network architecture diagram to illustrate the high availability setup.	
DCH/TR/29.06	High Performance The proposed data protection solution should support hardware cryptographic acceleration including • Intel and AMD AES-NI SPARC encryption IBM P8 cryptographic coprocessor	
DCH/TR/29.07	Data Access Audit and Report • The proposed data protection solution should provide fine-grained auditing records that show system accounts and processes accessing data based on security policy. • The proposed data protection solution should support integration with SIEM solution include: Archsight, Splunk, IBM Qradar, and deliver centralized access audit and monitoring report	
DCH/TR/29.08	Certification & Validations • The encryption key manager should be Common Criteria (ESM PP PM V2.1) certified • The encryption key manager should have option with FIPS 140-2 Level 1, FIPS 140-2 Level 2, FIPS 140-2 Level Certified	
30	**Tape Library**	
DCH/TR/30.01	Shall support Native data capacity of 100TB (uncompressed) expandable to 200TB (compressed).	
DCH/TR/30.02	Shall be offered with Minimum of four LTO6 FC tape drive. Drive shall support encryption.	
DCH/TR/30.03	Shall be offered with minimum of 48 Cartridge slots and scalable to minimum 100 Cartridge	
DCH/TR/30.04	Tape Library shall provide 8 Gbps native FC connectivity to SAN switches.	
DCH/TR/30.05	Library shall be able to back up the encrypted keys in a redundant fashion	
DCH/TR/30.06	Tape Library shall provide web based remote management.	
DCH/TR/30.07	The library should have cartridge I/O slots for secure & easy off-site backup storage	
DCH/TR/30.08	Tape Library shall have GUI Panel, shall be rack mountable and shall have option for redundant power supply	
DCH/TR/30.09	Should support industry leading backup software	
DCH/TR/30.10	40 LTO6 barcode labeled cartridges & 4 cleaning cartridges from the tape library OEM to be provided	
31	**Other requirements**	
DCH/TR/31.01	Provide ability to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for regulatory compliance and forensics	
DCH/TR/31.02	Email security	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	• Virus and Spam Protection (included with every Hosted Exchange mailbox) Spam and viruses can cripple a business • Email Archiving • Encryption (optional)	

GIS Software requirements:

GIS Enterprise Solution – Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
GIS/FR/1.01	MSI shall integrate all spatial & non-spatial data of this project into an Enterprise Geodatabase and develop a GIS portal with required GIS functions, Tools, Analysis & Dashboard to provide web access to all users of the project	
GIS/FR/1.02	MSI shall supply & deploy GIS Server software/engine and publish maps to all users of project.	
GIS/FR/1.03	MSI shall be responsible for appropriate geo referencing & geo tagging on the map covering all relevant assets like Wi-Fi Hotspots, bin locations, CCTV locations, street poles, etc. EPC Contractor to provide layers of all components being implemented to the MSI. MSI shall incorporate these layers in the overall GIS solution	
GIS/FR/1.04	MSI shall provide GIS engine that shall allow operators to get an overview of the entire system and access to all the system components dynamically. GIS engine shall enable dynamic view of the location and status of resources and objects/sensors	
GIS/FR/1.05	System shall enable authorized user to open a new incident and to associate the incident with its geographic location automatically, via GIS display	
GIS/FR/1.06	MSI shall carry out application development to functions & tools as per requirement	
GIS/FR/1.07	Data Design, Modelling and Services: • MSI shall finalize the data list with all its structure & metadata for approval; • MSI shall carry out data integration requirement study with stakeholders and submit SRS (System Requirement Study) and Architecture document for approval by considering following factors (not limited to): - Best GIS practices shall be followed in spatial positional accuracy, GIS layers overlay matching accuracy, data correctness and completeness; - All the data generated, stored, linked as a part of this project from various modules shall be available as necessary to integrate with GIS portal through web services or data sharing through live/real time, offline, periodical, etc. as deemed to be appropriate; - Apart from other modules data, all other required data for GIS portal shall be carried out with suitable data design and data modelling; - All required Data Modelling, Design shall be carried out by MSI to get Design Document approved from Rourkela Smart City; - Scale of mapping shall be 1:1000 or better as per requirement; - Integration of Government-to-Customer (G2C), Government-to-Government (G2G) & Government-to-Business (G2B) data; - Integration, export & import of various formats of data such as KML, JSON, XLS, XML, etc.;	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- 3D Data of city. • MSI shall carry out collection of data from various agencies or Government departments. All required data (spatial and non-spatial) are to be arranged by MSI. Rourkela Smart City will help by issuing required authorization letters; • Data creation - Necessary Field Survey, collection from various sources, compilation, digitization, accurate geo-referencing of spatial & Image data, migration, data conversion, integration, Enterprise Geodatabase preparation (in any OGC format) & maintenance shall be carried out by MSI; • MSI shall be responsible for identifying Data Gaps & take necessary measures & tasks to complete the data; • It is responsibility of MSI regarding required Data Quality, Correctness & completeness. MSI shall follow standard QA-QC practices in data management; • Some of the Government department's original records/drawings/maps/files may not be shared outside their office premises because of classified information, security & safety concerns. In such cases, the MSI shall compile/extract those source information at respective departments premises/onsite with necessary operational setup at their own expenses; • After successful Go-live and implementation, the Maintenance & Operation of GIS shall be carried out during MSI's contract period by taking care of Data Management, 24/7 availability of Database, periodical data updation, editing & performance management.	
GIS/FR/1.08	Should be capable of integrating with existing GIS data available with RSCL/ State Government/ RMC/RDA.	
GIS/FR/1.09	MSI shall deploy/install GIS Engine (GIS Server Software) on Client provided data center facility. It should have advanced GIS tools/ functionalities, capabilities and allow development of powerful GIS applications for GIS based information sharing, planning and Decision Support along with integration with Enterprise system;	
GIS/FR/1.10	GIS platform should provide the means to create, organize, secure, and manage geographic assets. As a centralized portal, it shall provide a single gateway interface and capabilities for all map based web services, data management, visualization and analysis	
GIS/FR/1.11	This Application should enable users to view multiple data layers on a map and perform various advanced functioning like map navigation, search, query, data analysis, geo processing, printing. It should support high scalability, security, availability, OGC Services of Open & Inter Operable standards and should be Industry standard Technology	
GIS/FR/1.12	Deployment of GIS Server Engine (Software) with Performance settings, Server settings, Hardware & Software performance settings, Security settings, Administrative roles/privileges settings, Role based functionality access for 3 to 4 levels, RWD (Responsive Web Design) settings, etc.	
GIS/FR/1.13	MSI shall be sole responsible for creating an integration approach through integration service bus for message delivery, services based on standards such as SOAP, HTTP and WCS	
GIS/FR/1.14	The integration service bus shall be designed to promote high throughput, compatibility, flexibility and scalability. Specific functionalities need to be configured for data retrieval from Web-GIS	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
GIS/FR/1.15	Shall provide a simple and easy to manage integration architecture for all external applications and should have functionalities to check for integrity and validity of data during import & export	
GIS/FR/1.16	Solution should be compatible with various open standards and technologies and should not restrict RSCL in using the solution data for any other applications, and should compliance National Data Sharing and Accessibility Policy (NDSAP)	
GIS/FR/1.17	Standardization and Interoperability – the proposed Web GIS Map engine shall be OGC (Open Geospatial Consortium) and SWE (Sensor Web Enablement) compliant	
GIS/FR/1.18	The client side user interface & map display Performance shall ensure real-time response (within 2 sec) at any given point of time & ensure uninterrupted performance; • The web user interface for the GIS map shall allow basic functionalities including (but not limited to) zoom factor/scale based feature loading, variable symbology, linetype scaling, cartography standards, etc.; • The system should have secured access; • Efficient search tools & print tools; • Efficient query tools – Spatial Query & non-spatial query; • 3D view options of buildings & terrain; • Role based access allowing various functionalities at different roles.	
GIS/FR/1.19	GIS base map shall include following, but not limited to these data with attributes which shall be finalized during study phase; • Road Network • Rail Network • Administrative Boundaries • Building footprints and names • Points of Interest data, not limited to: - Health Services (Hospitals, Blood Banks, and Diagnostics Centre, Ambulance Services, Other Medical Services etc. - Community services (Fire stations, Police stations, Banks, ATMs, Post offices, Educational facilities, Govt. Buildings etc.) - Business Centres (Shopping malls, Markets, Commercial complexes etc. - Residential areas (Apartments, Housing societies) - Transportation (Bus stops/Terminus, Parking areas, Petrol Pumps, Airports etc.) - Recreation facilities (Restaurants, Theatres, Auditoriums etc. - Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations • Land-Cover (Green areas, Open areas, Water bodies) • Address Layers (Pin code, Locality, Sub-Locality etc.) • Utility Networks (OFC, Water, Sewer, Drainage etc.) • Locations of other Municipal Assets • Education (Primary/Secondary/High School/Colleges) • Religious structures • Community centres	
GIS/FR/1.20	Detailed system requirement study, architecture & design shall be carried out with project stake holders and get approvals from client by considering following factors (not limited to):	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	• Enterprise level Architecture, Design & Development; • Service Oriented Architecture, Scalability, Interoperable standards and Agile development; • User Experience with portal; • Web Design and Content Management: Innovative or latest proven trends of Graphics design, Web pages, UI buttons & Tools development; • Real time performance of portal at user end; • User friendly & Interactive interface: Innovative UI Techniques, Easy & minimum clicks based operation by users, Scale, zoom factor based Map features display, Best practices of map features display, advanced techniques of features & symbols display management; • Map cartography - International standard shall be followed in terms labelling, color, linetype, Aesthetics, Symbology, Feature overlap management, etc.; • Development of Functions, Tools, Analysis, Dashboard; - Shall facilitate to create, delete & modify different Enterprise GIS Users Shall be accessible only to System Administrator while all other modules/sub modules shall be accessible to individual users based on the access rights provided to them by System Admin - Create Application Interface - Create admin right and grant suitable viewing/ data editing rights - Monitor access rights to user departments - Maintains Application Security - Shall allow Active Directory, LDAP, or other security source - Shall allow administrator to configure security to map service, layer and attribute levels - Shall allow group based security policies - MSI shall suggest firewalls that natively support all protocols required between the various servers (database, application and web) in the package. No special configuration shall be required to configure the firewall - Any changes to data should be recorded in a separate table and should be stamped with the identity of the user/program and the date / time of the creation/ change • The application should have all the map browsing functionalities implemented, including Descriptive Map Information Tool • Development of customized redlining capabilities; - Shall allow users to draw simple shapes (point, line, rectangle, polygon and circle) and add text to make annotations and markups to the map that should be printable. It shall allow the user to provide supplemental information on the map - Shall allow user to set the redlining display style based on the following specification: Line: color, style, transparency and width. Rectangle, circle, and polygon: fill color, fill opacity, outline style, outline color and outline width • Shall have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute, and also allow user to email map as an attachment	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	• Ability to connect to Data Stream: Connectors for common data streams including in-vehicle GPS devices, mobile devices, and social media providers • Process and Filter Real-Time Data: Detect and focus on the most important events, locations, and thresholds of operations without interruption. (data transmission without latency) Should be able to accommodate multiple streams of data flowing continuously through filters and processing steps that you define. (live event route mapping) • Monitor Assets: Track most valuable assets on a map. Should be able to track dynamic assets that are constantly changing location (such as vehicles), or stationary assets, such as weather and environmental monitoring sensors. • Respond to Events in Real Time: When locations change or specified criteria are met, automatically and simultaneously send alerts to key personnel, update the map, append the database, and interact with other enterprise systems. Alerts can be sent across multiple channels, such as e-mails, texts, and instant messages • Development of customized advanced analysis, query, search and report generation functions as per requirement by Enterprise level integration with various systems. Implement customized spatial analysis, weightage based thematic analysis, Spread analysis, Neighborhood analysis, required real-time geo-processing, Thematic mapping functions, etc. followed by generation of user friendly reports; • Web Services: Development and Enablement of Web Services for integration with external systems and access by external systems; • Development of Mobility Solutions, Mobile Apps, Web Apps and Location Analytics; • One-stop-shop or single point of interface for users of project with regard to access of all project implementations & features; • Integration & Development with Crowd sourcing, Social Media, Mobile & other Internet trends; • Development of any sub systems and portals for ease of use; • Integration of G2C, G2G & G2B functions; • Integration, Export & Import of various formats of data such as KML, JSON, XLS, XML, CSV, GPS data, etc. with external systems; • All Security aspects are considered for development; • All required web interface Modules and Sub-modules shall be planned & designed as per requirement.	
GIS/FR/1.21	Specific Web portal capabilities to be included as functional features: • Facility for display of spatial layers, query management like have various query tools for queries based on attributes, location, etc. • Integration of G2C, G2G & G2B functions; • Facility for basic Navigation tools like the software should have tools to Pan, Zoom, and Rotate the Map according to user requirements • Facility for spatial data classification based on specific attribute value and report generation • Ability to search and to zoom into the user specified x, y coordinates • Provision for definition of map projection system and geodetic datum to set all the maps in a common projection and scale.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	• Facility to click on any feature of the map and return a select set of attributes for feature. • Facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road widening impact on adjacent land. • Allow user to open raster images, or satellite images of various standard format. • Ability to import / export data from / to various formats like shape, MIF, dxf etc. • Allow users to export query results to various file formats like bmp, Tiff, Jpeg, pdf, etc. • Support printing spatial data at different scales and at adjustable print quality. • ODBC compliance enabling interface with leading industry RDBMS should be there. • Allow user to create layers or shortcuts to geographic data that store symbology for displaying features. • Provision of hyper linking the GIS feature as well as its attribute fields with existing documents, drawing files or scanned maps related to that feature. • Facility to create and organize user desired number of Spatial Bookmarks and should be able to share the same. • To have Control environment, feature functions, spatial relationship and geometric functions including math's and transformation functions • The software should support Map Services, Open Geospatial Consortium, Inc. (OGC) services like WMS, WFS etc. • The Application shall be able to serve multiple maps/layer with single/fewer configurations or shall have support for SQL Views • The application Shall have support for CQL Filters to obtain better Analytical capabilities • The WebGIS Application shall be highly scalable to serve increasing number of user with no extra cost • User should be able to see the location of CCTV cameras installed and mapped on to the GIS map • System should have provision to integrate with video feeds available from CCTV camera	
GIS/FR/1.22	Other Miscellaneous features to be incorporated (not limited to): • Editing Support role based multi-user editing access and editing work flows • Select features such as bookmarks, one-web functionality • Generation of thematic maps on-the-fly based on attributes details available in the GIS layers • Provision to store audit trial of user activities performed on the application • Web Development shall be done with best practice programming language and web development; • Integration with external system such as State Remote Application Centre, State Disaster Management System, etc., if required; • Integration with Open Data System; • Manage complete operations and maintenance of the developed application and ensure that the developed application is bug / error free, running smoothly and simultaneously incorporate necessary changes in the application functionality;	

Unified Communication System

The city has envisioned the need for an integrated incident dispatch and interoperability solution, which will help multiple agencies operating in Rourkela, to communicate with each other and take quick decisions to control the situation (integrated with ICCC platform). Solution should allow users from different communication devices or departments like existing push to talk radios, Mobile phone, land Line phones, PC/ web based clients, etc. to communication with each other. This Solution should help ICCC operator to have a real-time control and view of situations.

MSI needs to conduct a detailed assessment of communication devices used by different agencies, design a comprehensive technical architecture, implement and operate unified communication solution.

UCS – Minimum Functional Requirements

Sr. No	Functional Requirement	Compliant (Yes/ No)
UCS/FR/1.01	Integrates disparate push-to-talk systems with other voice systems for incident dispatch personnel.	
UCS/FR/1.02	Integrates server, routing, and IP communications elements to provide on demand incident communications across multiple groups.	
UCS/FR/1.03	Enables users to monitor and coordinate emergency response across incompatible radio systems and between multiple agencies and departments.	
UCS/FR/1.04	Extends existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate in an event.	
UCS/FR/1.05	As PTT base station radios will be physically integrated with in datacenter so there is no requirement to replicate this solution in DR.	
UCS/FR/1.06	The system shall be capable of integrating with multiple radio systems of different frequencies and protocols such as P25, TETRA, UHF, VHF and others.	
UCS/FR/1.07	The system shall have a patching function to enable patching of different radio and other audio end points together.	
UCS/FR/1.08	The system shall provide a powerful and easy-to-use Web interface: Authorized personnel shall be able to access the server from any location by using a supported browser and a network connection.	
UCS/FR/1.09	The system shall provide the dispatcher the ability to simultaneously select multiple channels at the same time to make a dispatcher outbound push-to-talk to all selected channels.	
UCS/FR/1.10	The system shall create virtual talk groups (VTGs) to facilitate Push-to-talk (PTT) communication between users of multiple types and technologies of Land Mobile Radios with users of desktop PCs, landline phones, cellular phones, smart phones, and IP phones.	
UCS/FR/1.11	The system shall utilize cluster redundant servers on the main authenticating server and media servers to provide high availability (HA) with no single point of failure. If a primary server fails, the other servers shall take over the load without communication interruption. The main servers and media servers shall be geographically separated or located together in the same data center.	
UCS/FR/1.12	The system shall have (N+1) redundancy. N+1 redundancy is a form of reliance that ensures system availability in the event of component failure. The servers will have at least 1 independent backup component. When a server is lost such as a media server the system just loses capacity.	
UCS/FR/1.13	The system shall provide a Loop Prevention mechanism to prevent creating a channel loop that causes audio feedback into the communication path when multiple channels are patched together. The system should automatically identify potential audio loops and resolve them before they cause any audio issues so that audio channels and talk groups shall remain clear without feedback.	
UCS/FR/1.14	The system shall provide radio pooling to enable the system administrator to group radio assets together into logical radio pools.	
UCS/FR/1.15	Dispatchers shall be capable to select / unselect specific channels or talk groups.	
UCS/FR/1.16	The system shall provide a web service API to integrate with third party applications, such as Command and Control systems, Physical Security Information Management (PSIM) systems and Computer Aided Dispatch (CAD) applications.	

Sr. No	Functional Requirement	Compliant (Yes/ No)
UCS/FR/1.17	The system shall provide an Incident Management administration console to provide a Web-enabled, easy-to-use interface for orchestrating communications across devices, technologies and locations.	
UCS/FR/1.18	The system shall enable the dispatcher to combine resources, including users and channels, to create Virtual Talk Groups (VTGs) and be able to quickly add or remove resources depending on incident status.	
UCS/FR/1.19	The system shall support role-based management to provide compartmentalized functions for personnel who need to perform different roles. A role assigned to personnel should define access privileges. The system shall be able to change user profiles at any time. The following roles, including an "all roles" assignment, shall be supported: 1.System Administrator 2.Operational Views Administrator 3.Operator 4.Dispatcher 5.User	
UCS/FR/1.20	The system shall provide license management: The administrator shall be able to use the Web-based interface of the server to manage system feature licenses and to support upgrades or feature additions.	
UCS/FR/1.21	The system shall provide an audit trail for analysis and operations management. Detailed activity logging shall enable administrators to determine which user actions were performed and when they were performed.	
UCS/FR/1.22	The system shall provide security features including a hardened Linux operating system for servers, strong passwords, password expiration, and user account lockout after the maximum number of invalid login attempts.	
UCS/FR/1.23	The system shall perform audio mixing functions through a Linux-based application server that is scalable. The HA servers shall be geographically separated or located together in the same data center.	
UCS/FR/1.24	The system shall provide user talker priority and pre-emption from individual mobile clients. The user priorities shall be set by the server or enable users to change their priority based on administrative privileges. The user with a higher priority shall have the ability to interrupt users on a channel with lower priority.	
UCS/FR/1.25	The system shall provide the ability for up to 10 talk lines to be added to a scanning virtual talk group. The scan virtual talk group shall send active audio to mobile clients that have access to the scan virtual talk group. The mobile client shall have the ability to transmit on the last audio talk group received without user's selecting the active channel. The mobile client user shall have the ability to manually select a talk group to transmit back on regardless of the last active channel.	
UCS/FR/1.26	The system shall have the capability of creating a broadcast virtual talk group. The broadcast virtual talk group shall add talk lines for an outbound audio transmission to all lines in the broadcast virtual talk group. The broadcast shall preempt any active audio on the talk lines in the broadcast group. The broadcast group can be created by a user with proper permissions from the mobile client software or from an administration console.	
UCS/FR/1.27	The system shall have the capability of making point to point push-to-talk calls or private calls between smart phone clients. Receiving users of a private call shall have the ability to accept or reject a private call.	
UCS/FR/1.28	The system shall have the capability of having a contacts directory that can be shared among all mobile client users in the system. The active contacts that are logged onto the system shall show an active presence in the contacts directory.	
UCS/FR/1.29	The system shall have the ability to view online users through an easy to use presence feature. Users on the channels shall have a viewable name and online status symbol. The users not on the channel shall be seen by changing the view from an online to all user click of a button.	
UCS/FR/1.30	The system shall enable integration with Microsoft Active directory or any other LDAP to enable login for dispatchers and mobile clients.	
UCS/FR/1.31	The system shall have the ability to authenticate between all servers connecting to the system using certificated-based PKI methods.	

Sr. No	Functional Requirement	Compliant (Yes/ No)
UCS/FR/1.32	The system should support an E&M interface to radio systems. For radio systems with a serial interface such as TETRA PEI, the system should be able to support the serial interface to control radio channels on the respective radio system.	
UCS/FR/1.33	The system server software should have the ability to run on bare metal or in virtualized environments.	
Operational View		
UCS/FR/1.34	Resource sharing across departments: Participants can share agreed-upon resources, such as channels or dispatchers, across operational views to facilitate collaboration among departments or locations.	
UCS/FR/1.35	Preservation of department ownership boundaries: Operational Views enables departments to create separate operational views for their own resources, sharing resources only as needed for incident response.	
UCS/FR/1.36	Extension of functions: Multiple virtual instances of software can reside on the same server, enabling departments to share common server hardware while still being able to control and manage their own resources.	
UCS/FR/1.37	Centralized management: The administrator can manage all operational views from the same interface.	
UCS/FR/1.38	Incident escalation between operational views: When a dispatcher is shared among operational views, the dispatcher receives the authority to share other resources, such as radio channels or other dispatchers, as needed for effective incident response.	
UCS/FR/1.39	Notification Alerts: The administrator shall have the ability to set up notification alerts from mobile clients for such events as: fall detection, impact detection, emergency alarm and informational alerts. The system shall support categorizing the alerts by severity, example 4 categories of alerts: major, minor, emergency, and informational. The different categories may have a different alerting capability. For example, when a user on the mobile clients pushes the emergency alarm all the notified users on the notification talk group or in the system shall get the emergency alarm on the dispatch console or on the other mobile users in the notification group. In the emergency level the user that initiated the emergency shall have the highest talker priority on the channel and preempt lower periodicity users on the system. Once the emergency alarm is cleared then the talker priority should go back to normal. Instant Messaging Integration: Each channel on the push-to-talk system shall have an associated instant messaging room where people behind the desk or dispatchers can type message into the room and have this message show up on the mobile clients. The mobile clients shall have the ability to type back to these messages and be seen by all the users on that talk group. Integrated phone and PTT: The system shall support the ability for mobile clients to be on the push-to-talk channels and make phone calls at the same time. This enables two simultaneous audio streams to be heard on the mobile client. The mobile client shall provide an easy way to mute the phone call user, the PTT channel, or mute completely for privacy concerns.	
Policy Engine		
UCS/FR/1.40	Invite notifications**:** Dispatchers can quickly invite users to join a Virtual Talk Group (VTG) with an Invite Notification. The dispatcher can select some or all members of a VTG and, at the touch of a button, initiate an action to notify or dial participants.	
UCS/FR/1.41	Integrated telephony interface: This feature enables personnel using landline and mobile phones to join a VTG, PTT interoperability conference between disparate land mobile radio systems, PSTN phones, IP phones, Mobile smartphones and PC clients.	
UCS/FR/1.42	Multipurpose policies: Can define flexible, powerful; multipurpose polices using an intuitive, web-based interface. Multipurpose polices enable organizations to pre-program frequently used or pre-planned communications strategies into standard operating procedures.	
IP-based dispatch console client		
UCS/FR/1.43	The dispatch console shall have UI client over Microsoft Windows program or Linux/Unix with latest version of OS support.	

Sr. No	Functional Requirement	Compliant (Yes/ No)
UCS/FR/1.44	The Dispatch Console shall be an end-to-end radio dispatching solution designed for mission-critical radio communications.	
UCS/FR/1.45	The dispatch software shall run on a standard PC platform, and extend existing push-to-talk (PTT) radio channels so that users with a variety of communication devices can participate in incident communication.	
UCS/FR/1.46	The Dispatch Console shall provide control of radio resources through an on-screen interface.	
UCS/FR/1.47	It shall enable users to monitor and coordinate emergency response across incompatible radio systems and between multiple departments and agencies.	
UCS/FR/1.48	It shall have a separate tab for Virtual Talk Group's, Policies, and Incidents.	
UCS/FR/1.49	It shall show user presence of all active mobile phones logged into the system.	
UCS/FR/1.50	It shall have a multi-line dialer where each dispatcher can patch up to 10 phone calls to channels.	
UCS/FR/1.51	It shall have a directory for phone number lists. There shall be a global, local, and personal list (associated to that user only).	
UCS/FR/1.52	It shall have the ability to tear away the parts of the Graphic User Interface (GUI) so that they can be dragged to other screens. The dispatcher shall have a function to restore the screen to the original setting where all the functions are in one application screen.	
UCS/FR/1.53	It shall have the ability for dispatchers to join cross mute groups enabling dispatchers not to hear one another when they are in close proximity range. The user interface shall show when the muted dispatchers are talking but not being heard through the active channel.	
UCS/FR/1.54	The GUI shall provide access to all dispatch features, including: • PTT and monitor up to min. 40 talk groups per Console position • Channel patching • Integrated telephony client for incoming and outgoing calls • Radio to telephone patching • Receive and transmit on-screen indicators for channel activity • Handset, headset, or desktop microphone operation • Individual channel mute/All mute • All talk • Instant recall recording per channel • Alert tones • Channel multi-select • Unit ID/talker ID • Emergency alert/acknowledge • Coded/clear channels	
UCS/FR/1.55	The dispatch console shall provide rich media incident management support, giving dispatchers the ability to consolidate information relating to an incident and instantly share it among participants, enabling the sharing of multimedia data such as the following: • Live video sent from surveillance cameras and mobile clients • Archived videos such as YouTube • Photos • Alarm monitoring • Journal and live statuses • Website links to resources such as standard operating procedures and maps	
UCS/FR/1.56	The Dispatch Console shall integrate with any analog or digital radio system, enabling dynamic any-to-any PTT communications.	
UCS/FR/1.57	The Dispatch Console shall provide mobility so that the user can login from any PC connected to the IP network.	
UCS/FR/1.58	The Dispatch Console shall have the ability to see alerts and respond to the alerts. This includes the ability to acknowledge the alert which turns off the audible indication. And the ability to clear the alert which turns off the visual notification.	
UCS/FR/1.59	The Dispatch Console shall have the ability to see a live map showing all the GPS coordinates of the mobile clients in the system.	

Sr. No	Functional Requirement	Compliant (Yes/ No)
UCS/FR/1.60	The Dispatch Console shall have the ability to type an instant message which will be sent to all the users on the channel. This includes the mobile client users as well as other dispatchers	

Sr. No	Functional Requirement	Compliant (Yes/No)
Android and Apple-based mobile client that supports the following functions		
UCS/FR/1.61	Access incident-related PTT channels to communicate between responders and radio users.	
UCS/FR/1.62	Support for up to min. 2000 active mobile users on the same system	
UCS/FR/1.63	Support up to min. 1000 active users in a single talk group.	
UCS/FR/1.64	Ability to have a user talker priority to assign to the mobile client.	
UCS/FR/1.65	Ability to change the mobile client talker priority with the proper privilege.	
UCS/FR/1.66	Ability to preempt calls or transmit audio over users of lesser priority or muting those audio transmissions of lower priority users.	
UCS/FR/1.67	Secure User Name and Authentication enabling users to log in to one or many systems using a server address, user ID and password.	
UCS/FR/1.68	Display authorized talk lines in a list format with a graphical icon show if it's a Virtual Talk Group, Channel, Talk Line or Incident.	
UCS/FR/1.69	Select Authorized talk line- once the user selects the talk line it must be make a connection to the selected talk line.	
UCS/FR/1.70	Operations Screen- The user shall have an easy to use operation screen that shows a button to be used for push-to-talk (PTT) service. The button shall be easily accessible from bottom of the screen of the mobile client.	
UCS/FR/1.71	The push-to-talk function should be supported with Android phones which have a programmable button such as a Sonim XP7 phone.	
UCS/FR/1.72	Full Duplex or Half Duplex operations: when a user presses the PTT button and there is activity from another user on that channel the original user should hear that audio in the full duplex mode. When a user presses the PTT button and there is activation from another user on that channel the original user should not hear that audio in the half duplex mode.	
UCS/FR/1.73	The user shall be able to select between internal or external speaker and microphone modes.	
UCS/FR/1.74	The users shall have access to a setting screen where they can easily change user settings. The settings screen shall enable the user the ability to change talker priority, microphone amplification, speaker gain, continuous PTT time out parameter, full duplex/half duplex mode, and audio prompts (on/off).	
UCS/FR/1.75	The mobile client shall have the ability to administer talk lines which include adding a new talk line, adding users to the talk line, adding virtual talk groups, adding scan groups, and adding broadcast groups.	
UCS/FR/1.76	The mobile client shall support simultaneous PTT and phone calls at the same time.	
UCS/FR/1.77	The mobile client shall support live mapping of all the mobile client users on the channel while still being on the main push-to-talk screen with an on-screen PTT button.	
UCS/FR/1.78	The mobile client shall support the live status of all the users on the channel. The status is online users and offline users. The user can toggle between the online and offline users.	

Sr. No	Functional Requirement	Compliant (Yes/No)
UCS/FR/1.79	The mobile client shall support the alerts feature which include informational alerts, minor alerts, major alerts, and emergency alerts. Alerts can be triggered by an on-screen command in the alert menu, a drop of a phone (fall/impact) or an emergency button press. Upon the emergency alert the talker screen border shall turn red indicating that it is in emergency mode. The user priority shall also turn to an "e" condition showing that the user is now in emergency mode which enables their audio to preempt everyone's PTT audio on that channel.	
System Advance function		
UCS/FR/1.80	Mapping- The system shall track the GPS coordinates of each mobile client user in the system. The tracking shall show up on the dispatch screen as well as the authorized mobile client screens. The tracking shall be adjustable for communicating location data from the mobile client to the location server. The location server shall be virtualized and run in the data center on VMWare or equivalent.	
UCS/FR/1.81	Reports- The system shall have a reports server which can collect reports by users per location. For example, if we segregate users into North, South, East, and West: the reports server associated with the North location shall collect all the records for the North talk groups and users associated with the North region.	
UCS/FR/1.82	Work on IP-based wireless phones including those with built in PTT buttons	
UCS/FR/1.83	The user shall have the ability to select the talk line or choose the contacts to view the contacts lists. When the user selects the contact they shall have the function of seeing where the contact is on the map, doing a private PTT call, making a phone call to the user, or making a private instant message to the user.	
UCS/FR/1.84	Visual indication when the user joins a talk line which includes the name and ID of all the users on the channel.	
UCS/FR/1.85	Audible indication when a user pushes the PTT button.	
UCS/FR/1.86	Once a user selects the contacts folder they can choose a global directory, local directory or favorites.	
UCS/FR/1.87	Once a user receives an individual PTT call, the wireless phone shall make a visual and audible indication of an inbound call.	
UCS/FR/1.88	The user shall have the ability to answer or reject the incoming individual PTT call.	
UCS/FR/1.89	When a user answers the Individual PTT call, they will leave the group PTT call. After the individual PTT is over, the user that answered the PTT call will automatically reconnect to the group PTT "talk line" that was previously selected.	
UCS/FR/1.90	The system must have a notification server that sets up notification policies. For example, when user1 pushes the emergency alert button, user2-10 are notified of this alert. The system shall have 4 levels of alerts: Major, Minor, Informational, and Emergency. The alerts can be configured to have different actions. For example, for an emergency alert the mobile clients shall have a pop up window with the emergency audible tone. For informational alerts, there is just an indication in the alerts screen of the alert there are not pop ups or acknowledgements.	
UCS/FR/1.91	· Advanced Encryption- The system shall have end to end payload encryption using Secure Real Time Protocol (SRTP). Mobile clients shall log in and authenticate to a server on the outside of the firewall once authenticated then they will log into the system securely through a firewall eliminating the need for VPN software.	
UCS/FR/1.92	The system shall have the ability to connect to an Intelligent Voice Response engine enabling phone users to dial into talk groups or activate policies.	

Sr. No	Functional Requirement	Compliant (Yes/No)
UCS/FR/1.93	The system shall have the ability to monitor system activity using Zabix software-based monitoring for diagnostic conditions.	
IP-based desktop phone client for ICCC operator		
UCS/FR/1.94	The system shall enable PTT functionality on IP Phones, enabling users to communicate over and monitor broadcast of communication channels with a push of a button.	
UCS/FR/1.95	The system shall provide remote management, enabling the user to manage the Phone Client securely and remotely through the system Server. This includes configuration changes, new information or resources, privileges, and other updates.	
UCS/FR/1.96	The system shall support multicast connectivity audio.	
UCS/FR/1.97	The system shall include listen-only channels so that users with the IP Phone Client can monitor channels in listen-only mode even if permission to talk is not provided.	
UCS/FR/1.98	The system shall provide for the extension of traditional PTT networks to IP networks extending voice reachability from PTT radio or broadcast networks to IP Phones.	
UCS/FR/1.99	The system shall support multiple channel types so that users have communication access not only to PTT radio channels, but also to broadcast channels or VTGs made up of multiple channels and communication device types.	
UCS/FR/1.100	The system must be capable of uninterrupted communications should the system server be unavailable. IP Phone users must be able to continue to communicate over the selected channel and operate in an offline mode.	

EMS (Enterprise Management System)

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
EMS/TR/1.01	Overview	• In addition to hardware and software requirements as prescribed in this RFP, SI is required to also design size, supply, implement and maintain an Enterprise Management System (EMS). The EMS shall be able to support the proposed hardware and software components deployed over the tenure of the Contract. The EMS shall be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. The EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring.	
EMS/TR/1.02		• MSI is required to design, supply, install, customize, test, implement, rollout and maintain the EMS application and hardware as per the requirements of this RFP.	
EMS/TR/1.03		MSI is expected to provide EMS encompassing but not limited to the following functions: • Configuration Management • Fault Management	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Incident, Problem and Change Management • Asset Management • Remote Control • SLA Management & Monitoring • Performance Management • Monitoring Backup and Management • Event Management • Server, Storage and other Infrastructure Management • Monitor network components of the LAN & WAN • Network Link Monitoring • Other modules as required by MSI to meet the requirements of the RFP	
EMS/TR/2.01	Monitoring, Management & Reporting with Enterprise Management System (EMS)	The EMS system shall provide for the regular monitoring, management and reporting of the ICT infrastructure of the project assets installed in the respective operations centre as well as field locations. It shall be noted that the activities performed by the MSI shall be under the supervision of Purchaser. The EMS system shall have the following features including but not limited to and as well act as authoritative source for the same: • Availability Monitoring, Management and Reporting • Performance Monitoring, Management and Reporting • Helpdesk Monitoring, Management and Reporting • Traffic Analysis • Asset Management • Incident Management and RCA reporting. • Change and Configuration management.	
EMS/TR/3.01	Availability - Monitoring, Management and Reporting Discovery, Configuration and Faults	This part of the specification shall ensure the monitoring, management, and reporting parameters of availability like discovery, configuration, faults, service levels etc. including but not limited to the following: **Monitoring and Management** • The proposed system shall support multiple types of discovery like IP range discovery – including built-in support for IPv6 , Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices • The proposed system shall support exclusion of specific IP addresses or IP address ranges. • The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity. • The discovery shall be able to identify and model of the ICT asset. • The proposed system shall provide a detailed asset report, organized by vendor name and device, listing all ports for all devices. The proposed system shall provide sufficient	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant. • The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason. • The proposed system shall provide out of the box root cause analysis. • The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines. • The proposed solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise alarm when VM migrations happen between hosts. • The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP. • The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies. • The proposed system shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules. • The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & startup configuration, Upload configuration etc.	
EMS/TR/3.02		**Reporting** • The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links. • The proposed system shall able to perform real-time or scheduled capture of device configurations. It shall also provide features to capture, view & upload network device configuration. • The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy. • The proposed system shall be able to monitor compliance & enforce change control policies within the diverse	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes. • The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.	
EMS/TR/4.01	Service Level Agreement	For the SLA related to ICCC and other smart elements please refer to Volume 3 of the RfP **Monitoring and Management** • The proposed service management system shall provide a detailed service dashboard view in terms of the service levels applicable to each of the departments' offices, along with applicable SLA parameters. • The system shall provide an outage summary that gives a high level status for each service as well as the details and root cause of any outage. • The solution should support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectiveness and audit Trail to ensure accountability for the project. • The solution should have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Project • The system shall be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted. • The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). • SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated. • The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA shall be available. • The solution should accept Data from a variety of formats; provide pre-configured connectors and adapters. • The system shall be capable of defining and calculating service credit and penalty based on clauses in SLAs.	
EMS/TR/4.02		**Reporting** • The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR),	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time. • The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation. • Ability to generate reports on penalty and credit due, as per SLAs for all necessary components • Monetary penalties to be levied for non-compliance of SLA, thus the system should provide Service Level Performance Report over time, contract, service and more. • The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box. • The system shall display option on Services, Customer, SLA's, SLA templates. • The customer definition option shall allow associating a service or an SLA with a customer. • Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardization and governance of the project • Real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.) - Resource utilization exceeding or below customer-defined limits - Resource utilization exceeding or below predefined threshold limits	
EMS/TR/5.01	Performance - Monitoring, Management and Reporting	The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components.	
EMS/TR/6.01	Network Performance Monitoring, Management and Reporting	**Monitoring and Management** • The System shall have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offend-to- end Network performance & availability to define service levels and further improve upon them. • The system shall provide discovery of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity • The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The tool shall have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices • The proposed system shall use intelligent alarm algorithms to learn the behavior of the network infrastructure components over a period of time • The proposed system shall have the ability to issues pings to check on availability of ports, devices. • The Ping Monitoring shall also support collection of packet loss, packet QOS, packet errors Latency and Jitters during ping checks. • The proposed system shall automatically collect and store historical data so users can view and understand network performance trends. • The proposed system shall be capable of monitoring network delay and delay variation • The proposed system shall provide the ability to visually represent LAN/WAN links with displays of related real-time performance data including utilizations. • The proposed system shall provide customizable reporting interface to create custom reports for collected data • The proposed system should use advanced root-cause analysis techniques and policy-based condition correlation technology (at network level) for comprehensive analysis of infrastructure faults. • The proposed system shall be able to clearly identify configuration changes and administrators should receive an alert in such cases. • The proposed system shall support multicast protocols too, if the overall project solution offered includes multicast. • The proposed system shall support monitoring of Syslog or equivalent. • The proposed system shall provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings.	
EMS/TR/6.02		**Reporting** • The Network Performance Management console shall provide a consistent report generation interface from a single central console. • This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources • The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. • The proposed system shall provide the following reports for routers etc. as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out. • The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.	
EMS/TR/7.01	Application Performance Monitoring, Management and Reporting	**Monitoring and Management** • The proposed solution shall proactively monitor all user transactions for any web- application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes • The proposed solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer. • The proposed solution shall correlate performance data from HTTP Servers (external requests) with internal application performance data • The proposed solution shall see response times based on different call parameters. For example the proposed solution shall be able to provide CPU utilization metrics • The proposed Solution shall be able to correlate Application changes (code and configuration files) with change in Application performance. • The proposed solution shall allow data to be seen only by those with a need to know and limit access by user roles • The proposed solution shall measure the end users' experiences based on transactions • The proposed solution shall give visibility into user experience without the need to install agents on user desktops. • The solution shall be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer. • The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
EMS/TR/7.02		**Reporting** • The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction • The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the server room without having to rely on network monitoring tools. • The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.	
EMS/TR/8.01	Systems and Database Performance Monitoring, Management and Reporting	**Monitoring and Management** • The proposed system shall addresses management challenges by providing centralized management across physical and virtual systems • The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored. • It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system. • It shall also be able to monitor various operating system parameters depending • On the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds. • The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc. • The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started • The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to take action like sending an email. • The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console. • It shall be able to automate monitoring, data collection and analysis of performance from single point.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.	
EMS/TR/8.02		**Reporting** • The proposed system shall provide Performance Management and Reporting — Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines . • Role based Access — Enables role-based management by defining access privileges according to the role of the user. • The proposed Virtual Performance Management system shall integrate latest virtualization technologies	
EMS/TR/9.01	Traffic analysis	• The proposed system shall enable the server room to centrally manage user access privileges and allow deploying baseline security polices so that the right people have access to the right information. It shall proactively secure access to data and applications located on Linux, UNIX and Windows system servers • The traffic analysis system shall be from same OEM providing Network Fault & Performance Management System. • The tool shall support Flow monitoring and traffic analysis for NetFlow, J-Flow, sFlow, Netstream, IPFIX technologies or equivalent. • The solution shall provide a central web based integration point reporting and able to report from a single console across 100,000 interfaces. • The solution shall be of the type passive monitoring without a need to install any probe or collector for data collection. • The solution shall provide the following metrics: Rate, Utilization, Byte Count, IP hosts with automatic DNS resolution, IP conversation pairs with automatic DNS resolution, Router/interface with automatic SNMP name resolution, IPv6 addresses The proposed solution shall keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database shall have a maximum 15 minute window granularity without roll up. A user shall be able to select any 15 minute window over the last 12 months and display unique utilization and protocol data for every monitored interface. The proposed solution shall keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database shall have a maximum 1 minute window granularity. A user shall be able to select any 1 minute	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		window over the last 30 days and display unique utilization and protocol data for every monitored interface. All custom reports from the long term database shall support the ability to be run manually or scheduled to run automatically at user selectable intervals. The system shall allow via API for Excel to download data to generate reports. The system shall be able to restrict views and access for defined users to specific routers, interfaces, and reports. The user shall be able to generate reports from the long term database based on specific thresholds defined by the user where the threshold can be compared to rate, utilization or volume of every monitored interface as a filter for inclusion in the report. The proposed system shall be capable of automatically detecting anomalous behavior such as virus attacks or unauthorized application behavior. The system shall analyze all traffic and alert via SNMP trap and syslog of any suspicious activity on the network. The system shall provide the ability to group interfaces into functional groups based on any user criteria. The grouping function shall allow users to create group names and add interfaces into that grouping for reporting purposes. Once created, these groups shall be available for selection within custom reports as a mechanism to include multiple interfaces without individual selection for inclusion. The monthly view shall provide a graphical representation of the level of utilization for each fifteen minute interval of each day of the month. The user shall be able to easily change the data type of the main interface view to a tabular format showing the increase or decrease of traffic generated by that protocol as a percentage using discrete least-squares approximation to find a best fit line of growth	
EMS/TR/10.01	Asset Management through EMS	• Ability to provide inventory of hardware and software applications on end-user desktops, including information on processor, memory, OS, mouse, keyboard, etc. through agents installed on them • Ability to have reporting capabilities; provide predefined reports and ability to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs • Ability to provide the facility to collect custom information from desktops • Ability to provide facility to recognize custom applications on desktops • Facility for the administrator to register a new application to the detectable application list using certain identification criteria. Shall enable the new application to be detected automatically next time the inventory is scanned • Facility for User self-registration. • Ability to support configuration management functionality using which standardization of configuration can be achieved of all the desktops	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Software metering shall be supported to audit and control software usage. Shall support offline and online metering. • Ability to support dynamic grouping of enabling assets to be grouped dynamically based on some pre-defined criteria e.g. a group shall be able to display how many and which computers has a specific application installed. As and when a new computer gets the new application installed it shall dynamically add to the group • Ability to use the query tool to identify specific instances of concern like policy violation (presence of prohibited programs / games and old versions, etc.), inventory changes (memory change, etc.) and accordingly it could perform several actions as reply. These actions could be (a) sending a mail, (b) writing to files, sound an alarm (c) message to scroll on monitor screen if the administrator, etc. • Facility to track changes by maintaining history of an asset • Ability to have web based console The proposed EMS solution shall provide comprehensive and end - to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure. **Note:** It is mandatory that all the modules for the proposed EMS Solution shall provide out-of- the-box and seamless integration capabilities. SI shall provide the specifications and numbers for all necessary Hardware, OS & DB (if any) which is required for an EMS to operate effectively.	
EMS/TR/11.01	Incident Management and Root Cause Analysis Reporting	• An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process. • Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration. • It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed. • Testing shall be performed to ensure that recovery action is complete and that the service has been fully restored. • The SI shall keep the end users informed of the progress of their reported incident.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• When the incident has been resolved, it shall be ensured that the service desk records of the resolution steps are updated, and confirm that the action taken has been agreed to by the end user. Also, unresolved incidents (known errors and workarounds) shall be recorded and reported to provide information for effective problem management. • Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. • The SI shall conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's). • The incident management activities shall be carried out by the SI in such a way that an incident is resolved within the agreed time schedule. • Root Cause Analysis (RCA) shall be conducted by the SI. • Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.	
EMS/TR/12.01	Change and Configuration Management	• Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services. • All changes shall be initiated using change management process; and a Request for Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk. • The SI shall ensure that all changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes. • Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change shall be analyzed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement. • Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation. • The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures. • A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access. • The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI. • Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners. • Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable. • A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control. • Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, software and hardware configuration images.	
EMS/TR/13.01	EMS Ability to integrate with other services	The proposed EMS solution shall comply with key integration points out of the box as listed below but not limited to: • The proposed network management system shall integrate with the helpdesk system by updating the Asset with CI information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk. • The proposed network management system shall attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it shall be automatically created prior to submitting the ticket. NMS console shall show associated helpdesk ticket number for the alarms that generated those tickets. • SLA's violation on monitored end user response time shall open a helpdesk incident out of the box. • Proposed Application Performance Solution shall integrate with Network Fault Monitoring Solution to forward Application Performance Threshold violation alarms in proposed Network Fault Manager Console. • The proposed Fault Management Solution shall support integration with proposed help desk or trouble ticketing system such that integration shall Associates alarms with Service Desk tickets in the following ways: Manually creates tickets when requested by Fault Management GUI operators Automatically creates tickets based on alarm type Provides a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		Maintains the consistency of the following information that is shared between alarm and its associated Service Desk ticket including status of alarms and associated tickets and current assignee assigned to tickets. Helpdesk ticket number created for associated alarm shall be visible inside Network Operation Console. It shall be integrated in a way that Helpdesk incident can be launched once clicked on ticket number for associated alarm from within Network Operation Console. The proposed virtual performance management system shall integrate with proposed Network Management and Performance Management system out of the box. The proposed NMS shall provide unified workflow between the fault and performance management systems including bi-directional and context- sensitive navigation, such as Navigate from the Topology View to At-a-Glance or Trend Reports for any asset Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports Proposed Performance Management system shall feed in discovery from Devices already discovered in Network Management Module without starting discovery process again all together in Performance Management Engine this shall reduce effort of having to perform discovery on both Fault and Performance Management Engines .Discovery can be synchronized. Note: SI shall use Industry standard tools to ensure smooth/seamless integration and out of the box workability of the offered solution.	
EMS/TR/14.01	ICT Asset Hardening	All the ICT assets shall be hardened as per the Hardening guidelines and industry leading practices. Remove all unauthorized software, utilities, and services. All required logs shall be configured and monitored	
EMS/TR/15.01	Helpdesk	• The Helpdesk services should be in accordance to ITIL standards and should be running 24x7x365. MSI has to propose a setup hunting telephone lines for lodging telephonic service request, as well as an email ID, which is monitored 24x7x365. • Call Logging for queries / services / complaints (Trouble Ticketing) • Call logging will be through telephone / mobile, e-mail or service desk software or through personal messenger. • Proactive monitoring has to be done by service provider to reduce the resolution time in case of any link failure. Proactive monitoring should have mechanism of auto generation of link down request for faster resolution. Ticket raise information should be inform to RSCL and to central helpdesk for ticket resolution monitoring. • Recording redressal of complaints in the Service Desk Software, Call closure • Call Routing to respective vendors.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• Call Escalation for all the IT assets supplied under the purview of this contract to senior authority of MSI to be listed in the system, if call is not redressed by respective field representative of MSI. • Call monitoring which includes recording status of complaint redressal and reasons for not redressing complaint if any. • Incident Management • Call analysis and generation of reports using a computerized tool for uptimes and SLA's. • Help Desk shall follow up all the calls and perform audio recording calls so that SLA is not violated. • MSI shall keep ICCC team informed about the progress at regular intervals. Problems shall be classified into various levels of priority mentioned in the SLA. The assigned priority for each problem shall be dependent upon: - The extent of the problem's impact on the usability of the system - The percentage of project users affected by the system • The initial assignment of priorities is the responsibility of the Help / Service Desk's Problem Manager. However, RSCL can challenge the priority assigned to a particular problem and procedures that exist for escalating a problem to progressively higher management levels, until agreement is secured. The precise definition of problem priorities should be documented in MSI's problem management procedures. • Primary telephonic support (complaint / issue resolution) at Helpdesk where resources are deployed and field level support on a need basis. 15. Any other help / service desk related services not listed above but required for smooth functioning of help / service desk services as directed by the RSCL.	
EMS/TR/15.02		**Helpdesk - Monitoring, Management and Reporting** • The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface. • The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes. • Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools. • The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc. • Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		• The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users. • The proposed helpdesk system shall have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues. • The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types. • The proposed helpdesk system shall be capable of assigning call requests to tech al staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc. • The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window. • It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet. • Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket. • It shall allow IT team to create solution & make them available on the end – user login window for the most common requests	
EMS/TR/15.03		**Helpdesk- Integration with Services** • The helpdesk solution shall include VoIP based EPABX, IVRS, Automatic Call Distribution (ACD), Voice Logger Server among other hardware and software. Using the contact center solution, citizens can contact city administrator through the emergency communications system or through the helpdesk helpline number. • The helpdesk solution shall be able to route voice/ VOIP calls from centralized Interactive Voice Response System (IVRS) to respective call center (s) along with interaction history of the calling party. • IVRS shall support various means of Alarm indications in case of system failures, e.g. Functional error, missing voice message prompt, etc., and shall generate error Logs. • IVRS shall be able to get information /text/data from databases, convert to voice, and speak back to the caller in relevant/desired language. • Solution shall provide pre-integration with industry standard IVRS servers and enhance routing & screen pop by passing forward the information. Interactive Voice Response System (IVRS) should – - Play welcome messages to callers Prompts to press and collect Dual-tone multi-frequency signalling (DTMF) digits	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		- Able to integrate with backend database for self-service, as and when required - Offer GUI based tool to be provided for designing the IVR and ACD call flow. - Support VoiceXML for Automated Speech Recognition (ASR) and Text-To-Speech (TTS), and DTMF call flows - Able to Read data from HTTP and XML Pages be able to run outbound campaigns • Automatic call distribution (ACD) solution should – - Able to route the call to any remote call center agent using IP phones - Have an ability to queue or hold the call for an agent if none is immediately available - Have an ability to keep the callers informed as to the status of the call and providing information to callers while they wait in queue - Able to perform prioritized call routing e. be highly available with hot standby and seamless failover in case of main server failure - Support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups - Support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialled number etc. h. support call routing based on longest available agent, circular agent selection algorithms - Maintain log of all services offered which can be used for audit and analysis purpose. - Support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay - Allow agents to chat with other Agents or supervisor from the Agent desktop software - Allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop - Support Queuing of calls and playing different prompts depending on the type of call and time in the queue • System shall be able to integrate with e–mail / SMS gateway so that appropriate messages can be sent to the relevant stakeholders after the interaction and any updates thereon. • Shall intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents. • Solution shall provide Computer Telephony Integration (CTI) services such as:	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		- CTI link should allow a computer application to acquire control of the agent resources on the IP EPABX & change state of the agent phone through commands on the CTI link. - CTI link should pass events & information of agent states & changes in agent states as well as incoming calls to the computer applications. - CTI link should allow a computer application to take control of the call flow inside the IP EPABX & also allow the computer application to decide the most suitable action / agent for an incoming call. - Automatic display (screen pop) of information concerning a user/customer on the call agent - Screen prior to taking the call based on ANI, DNIS or IVR data - Synchronized transfer of the data and the call to the call centre agent - Transfer of data corresponding to any query raised by any agent regarding a query raised by ▪ A caller whose call is being attended by the agent ▪ Call routing facilities such as business rule based routing, skills-based routing etc. • Supervisor Module - The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features:- ▪ Any supervisor shall be able to monitor or control any group in the call Centre ▪ It shall show the live activity of each agent in details as well as in a summarized fashion including information like total number of calls received, calls answered, average response time etc. ▪ Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc. ▪ Live status of the group shall be shown, including waiting calls and calls being answered currently. ▪ Access to the supervisor console shall be restricted. ▪ It shall be possible for a supervisor to attend calls whenever necessary • Reporting - System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.	

S.No.	Enterprise Management System		Compliant (Yes / No)
	Parameters	Minimum Specifications	
		- Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes - Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents. - Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures. - Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV • Solution should offer audit trail with the following features – - Solution should have a comprehensive audit trail detailing every user activity including system/security administrators with before and after image - Audit trails presented by the system shall be very detailed with all the related fields, such as User ID, time log, changes made before and after, Machines ID etc. - It shall have the facility to generate security report(s) and audit the whole process from logs reports at any future date. The system shall have complete audit trail of any changes to the system e.g. alert generated, system configuration etc. - System shall not allow audit log to be deleted and any attempts to delete should be logged. - System shall have at a minimum following standard reports: ▪ List of users, user privileges and status of User sign-off and sign-on ▪ User violation – unsuccessful logon attempts - User additions, amendments and deletions with before & after image	

Data Centre: Non-IT Components

The data center shall meet tier 3 specifications in terms of redundancy and concurrent maintainability requirements.

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
1. Fire Proof Enclosure for Data Centre		
DCN/TR/1.01	Capacity: 2MX1MX3M	
DCN/TR/1.02	Temperature to Withstand: 1000° C for at least 1 hour	
DCN/TR/1.03	Internal Temperature: 30° C after exposure to high temperature For 1 hour	
DCN/TR/1.04	Locking: 2 IO-lever high security cylindrical / Electronic lock	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
2. Racks and PDU		
DCN/TR/2.01	19" 42 U Rack with necessary Accessories	
DCN/TR/2.02	Cable entry brush (rack bottom)	
DCN/TR/2.03	32A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor as per Rack layout	
DCN/TR/2.04	16A IP PDU with Ethernet based Environment Monitoring System with one Temperature Sensor	
DCN/TR/2.05	Blanking Panels	
3. Fire Suppression System		
DCN/TR/3.01	Comply with NFPA 2001 or ISO 14520 standard	
DCN/TR/3.04	Should have zero ozone depletion potential	
DCN/TR/3.05	Have a short life span in the atmosphere, with atmospheric life time of less than 5 days	
DCN/TR/3.06	Be efficient, effective and shall not require excessive space and high pressure for storage	
DCN/TR/3.07	Key components are valves and its accessories, actuators, flexible discharge and connection hoses, check valves, pressure switch, and nozzles	
DCN/TR/3.08	The hazard space volumes shall be protected from a common central or individual supply, the cylinder bank or individual cylinder system, with corresponding pipes and nozzle system.	
DCN/TR/3.09	The individual zone/ system shall be dimensioned to give a complete discharge of the agent in less than 10 seconds into the affected zone.	
DCN/TR/3.10	The software calculation shall be approved VdS or FM / UL. The discharge time shall not exceed 10 seconds. After end of discharge (10s) a homogeneous NOVEC 1230 concentration shall be built-up in the room.	
DCN/TR/3.11	The design concentration shall follow ISO 14520 or at minimum NFPA 2001 for under floor, room and ceiling space. Unless otherwise approved, room temperature for air-conditioned space shall be taken around 20□C. For non-air conditioned space, the temperature shall be taken around ambient temperature. The system shall be designed with minimum design concentration of 4.4 % as applicable to Class-A & C fire.	
4. Water Leak Detection System		
DCN/TR/4.01	Water Leak Detection Panel: • Alphanumeric LCD Display with the minimum of 3Lines • Soft Touch Membrane Keypad • LED Indication of the events like power, Alarm & Fault • Password protected event log facility • Remote monitoring via MODBUS/BACnet protocol • Configurable sensitivity adjustment • Dedicated Hooter output for local alarm	
DCN/TR/4.02	Water Leak Sensing Cable: • Should be mechanically strong, resistant to corrosion and abrasion • Shall be constructed with two sensing wires, an alarming signaling wire and a continuity wire constructed by fluoropolymer carrier • Shall have end circuit to detect open circuit fault	
5. Raised Floor		
DCN/TR/5.01	System: • Access floor system to be installed at finished floor height of maximum 600	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
	mm from the existing floor level. • The system will provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in an office / server / DCS / panel / rack area. • The entire Access floor system will provide for adequate fire resistance, acoustic barrier and air leakage resistance.	
DCN/TR/5.02	Panels: • Panels will be made up of inert material Calcium sulphate. The bottom of the panel shall be of Aluminium foil to create a fire and humidity barrier and this should provide floor's electrical continuity. Panels will remain flat through and stable unaffected by humidity or fluctuation in temperature throughout its normal working life. The Panels will be UL listed/FM/DM approved. • Panels will provide for impact resistance top surfaces minimal deflection, corrosion resistance properties and shall not be combustible or aid surface spread of flame. • Panels will be insulated against heat and noise transfer. • Panels will be of requisite height fully interchangeable with each other within the range of a specified layout. • Panels shall rest on the grid formed by the stringers which are bolted on to the pedestals. • Panels shall be finished with anti-static 0.9 mm Laminate and 0.45 mm thick plastic edge material that is self-extinguishing and will be PVC free	
DCN/TR/5.03	Panel Loading: • Concentrated point load: 450 Kg • Uniformly Distributed Load (UDL): 1500 Kg/M2	
DCN/TR/5.04	Fire Rating: • The Panels will confirm to class O and Class 1 Fire Ratings tested as per CIRC 91/61 or BS 446 Part 6 & 4 (60 min)	
DCN/TR/5.05	Pedestals: • Pedestal installed to support the panel will be suitable to achieve a finished floor height of 600mm. Pedestal design will confirm speedy assembly and removal for relocation and maintenance. Pedestal base to be permanently secured to position on the sub-floor. • Pedestal assembly will provide for easy adjustment of levelling and accurately align panels to ensure lateral restrain. Pedestals will support an axial load of 1500 Kgs, without permanent deflection and an ultimate load of 3000 Kgs. Pedestal head will be designed to avoid any rattle or squeaks.	
6. PVC Conduit		
DCN/TR/6.01	Please refer to section ICCC-NIT/TR/3.01 above	
7. Wiring		
DCN/TR/7.01	Please refer to section ICCC-NIT/TR/4.01 above	
8. Earthing		
DCN/TR/8.01	Please refer to section ICCC-NIT/TR/5.01 above	
9. Cable Work		
DCN/TR/9.01	Please refer to section ICCC-NIT/TR/6.01 above	
10. Air-conditioning		
DCN/TR/10.01	Please refer to section ICCC-NIT/TR/7.01 above	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
11. Fire Alarm System		
DCN/TR/11.01	Please refer to section ICCC-NIT/TR/9.01 above	
12. Aspirating Smoke Detection System		
DCN/TR/12.01	This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labor necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes. • Codes and standards - The entire installation shall be installed to comply one or more of the following codes and standards - NFPA Standards, US - British Standards, BS 5839 part :1 • Approvals All the equipment's shall be tested, approved by any one or more: - LPCB (Loss Prevention Certification Board), UK - FM Approved for hazardous locations Class 1,Div 2 - UL (Underwriters Laboratories Inc.), U - ULC (Underwriters Laboratories Canada), Canada - Vds (Verband der Sachversicherere.V), Germany • Design Requirements - The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter. - It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based. - The system shall allow programming of: – Multiple Smoke Threshold Alarm Levels. – Time Delays. – Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault. – Configurable relay outputs for remote indication of alarm and fault Conditions. - It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool. - Optional equipment may include intelligent remote displays and/or a high level interface with the building fire alarm system, or a dedicated System Management graphics package. - Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter. • Displays on the Detector Assembly - The detector will be provided with LED indicators. - Each Detector shall provide the following features: Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector/Smoke Dial display represents the level of smoke present, Fault Indicator, Disabled indicator • Sampling Pipe	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
	- The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards. • Installation - The Contractor shall install the system in accordance with the manufacturer's recommendation. - Where false ceilings are available, the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube. - Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval. - The bidder shall submit computer generated software calculations for design of aspirating pipe network, on award of the contract.	
13. Rodent Repellent System		
DCN/TR/13.01	Please refer to section ICCC-NIT/TR/10.01 above	

Disaster Recovery Centre

The Disaster Recovery Centre (DRC) will replicate all the servers in the DC. All the applications in the DC will be available in the DRC. Application level redundancy is not considered in the DRC. The storage at DRC shall be able to record the feed from all cameras for a minimum of 15 Days. The Data Recovery Centre will be the backup location for all application servers in the data centre.

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
DR/FR/1.01	The Disaster Recovery Centre Facility should be within India and should be Tier III or above. The DR site shall be located in Bhubaneswar	
DR/FR/1.03	MSI shall be fully responsible for upgrades, technological refreshes, security patches, bug fixes and other operational aspects of the infrastructure that is in the scope or purview of MSI	
DR/FR/1.04	MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security resources.	
DR/FR/1.05	In no circumstances, the data accumulated and processed by Command Control and Communication Centre should be compromised. Hence, provisions will be made to keep all the data stored in this platform highly secured with required multi layered security access control and authorization framework. Further the platform shall provide an open standards based integration Bus with API Management, providing full API lifecycle management with governance and security features.	
DR/FR/1.06	Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.	
DR/FR/1.07	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness	
DR/FR/1.08	All applications need to have high performance clustering (redundancy) within the Data Centre with automatic fail-over, and redundant data storage in active passive or active-active configuration as per the high availability targets. The data replication should be continuous among all the servers and shared storage should not be used. All mission critical systems should be active-active configurations. Active passive configurations may be permissible for supporting applications.	
DR/FR/1.09	The DRC shall have ISO 24001 or latest certification.	
DR/FR/1.10	The bidder shall provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with RSCL during the project kick off. • Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site. • Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site. • Operations from DR site: Ensuring secondary site is addressing the functionality as desired • Configure proposed solution for usage The service provider shall be responsible for – • Devising and documenting the DR policy discussed and approved by RSCL. • Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit	

Minimum Technical Requirements

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
DR/TR/1.01	MSI shall provide private connectivity between RSCL's network and DRC Facilities.	
DR/TR/1.02	Interoperability support with regards to available APIs, data portability etc. for RSCL to utilize in case of migration back to Local Data Centre, burst to a cloud service provider for a short duration or availing backup services from a Cloud service provider	
DR/TR/1.03	The proposed solution should offer a workflow based management & monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location	
DR/TR/1.04	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR	
DR/TR/1.05	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness	
DR/TR/1.06	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This should significantly reduce custom development of scripts and speedy deployment of DR solutions	
DR/TR/1.07	The proposed solution should facilitate workflow based switchover and switchback for DR drills for standard applications based on industry best practices	
DR/TR/1.08	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication	
DR/TR/1.09	MSI shall be responsible for providing Cloud service for storing all applications at DR at a location specified by RSCL [minimum 30% production capacity, RTO – 120 mins, RPO – 15 mins], which will be implemented for the project duration. The proposed cloud infrastructure should have not less than 100 cores. Each Compute node should have the latest generation processors containing not less than 128 GB of RAM. The cloud infrastructure should not provide not less than 25 TB for block storage and not less than 100 TB for object. The same can be augmented as per the future requirements. MSI has to design the DR solution as per the requirement of the RFP and factor the same in their technical and financial bid.	
DR/TR/1.10	RSCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for RSCL's applications. RSCL shall retain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.	

Network Connectivity on Lease

Objective

RSCL intends to procure leased circuits and internet bandwidth through the MSI for its citywide network from a telecom service provider. The MSI will select a suitable telecom service provider on competitive basis for meeting its connectivity requirements. The network, which will be provisioned through the MSI for SLA purposes through a tripartite arrangement on a Lease basis, will be entered into SLA agreement for ensuring seamless connectivity for intranet/Internet within the Rourkela Smart City systems. The agreed leased contract should provision network connectivity across all smart elements within the Rourkela city and other areas as defined by the RSCL from time-to-time. The internet services shall be extended, in all these cases with necessary security features fully applied. For all services outside of the RSCL and parts of the Odisha Government systems accessed through the Rourkela Smart City networks shall all be fully compliant to the required security protocols as envisaged by respective systems for data exchange / store / forward from the Rourkela Smart City network. The expected benefits to be derived from city network backbone are:

- To provide inexpensive and pervasive connectivity all across the city.
- To boost digital inclusion among departments and citizens.
- To provide 24*7 uninterrupted connectivity across the city
- To establish a medium for quick data gathering from multiple sources and faster decision making.
- To act as a channel for integration of all the city services.
- To enable the government to have advanced communication products/platforms and better security and surveillance systems seamlessly functioning through this network backbone.
- Band Width for converged networks, each individual application server is expected to have a minimum concurrency of 30,000 users while this could scale up, post implementation, to about 50,000 concurrent users during the Operations and Support phase of 5 years.
- The intranet bandwidth required will be on the basis of the connecting end point device capability for data feeds in to the ICCC etc. May vary from a simple 9600 Band to up to 1 Gbps depending on the nature of the connecting devices and the objectivity of the system.
- The external gateway internet services to all services outside of the RSCL owned systems shall be a minimum data rate multiplied by the concurrency of a minimum of 30,000 concurrent users with specified respective application pay loads (such as attachment of up to a maximum of 10 documents and/or images etc.).

Scope of work

The detailed scope of work for MSI for providing a pan city network backbone is given below. The MSI shall work seamlessly with the backend telecom service provider to meet these requirements.

- Provide lease circuit connectivity for supporting maximum 20 MBPS bandwidth at each node/ location in the network (including individual intersections/ junctions, sensor locations, etc.) and total bandwidth of minimum 12 Gbps for the entire network.
- It shall be the responsibility of MSI to provide/ arrange to provide all the last mile terminating devices including MUX, Modem, VPN Concentrators, Media Convertors, Routers, Power Backup for device, etc. to interconnect all points of use, origin of signals in the case of SCADA and all edge devices If any racks, wall bracket support and any other equipment as may be required shall also be MSI's responsibility.
- MSI shall study the existing setup and design the new WAN architecture under this project to meet the intended objectives and scope of pan city network backbone. MSI shall provide End-to-End connectivity to all field locations including the Special Sites and Data Center sites over Leased Circuits.
- Additionally, MSI shall also be responsible for providing connectivity for the sites which the RSCL intends to cover over the contract period, as and when RSCL feels the need.
- MSI shall be required to provide maintenance services for the WAN connectivity at all the sites covered under this engagement.

- As part of the preventive maintenance services MSI shall be required to maintain the upkeep of the medium of connectivity, reinstating the medium, any other maintenance job required to meet the redundancy and SLAs as stipulated in the RFP.
- RSCL may order an increase/decrease/termination/withdrawal in bandwidth, which MSI shall take into account.
- The network should be capable of providing bandwidth on demand for planned as well as for unplanned activities.
- MSI should provide the bandwidth for intranet & internet.
- The committed bandwidth has to be provided at all locations (Indicative locations of various sensors, cameras and other IOT devices has been indicated as part of various component details in this RFP). MSI shall have to calculate the requirement of bandwidth at each office/location/point of use or point of inter-connect required to connect to the Rourkela Smart City network. This calculated bandwidth shall be allocated to the RSCL on 24X7 basis.
- Adding new location – whenever a new location is decided to be added by the RSCL, an order will be placed with MSI at the contracted price. MSI shall carry out site-survey at new location for feasibility of location over wired connectivity. MSI would be required to implement and commission the location within 2 weeks from the date of work order.
- The network shall be a fully secured network which also connects to many real time interfaces including SCADA, annunciators, display and messaging systems, SMS alerts and emergency response activation protocol hierarchically with traceability features. Typically it could be a star – hub and spoke type network with multi-tier architecture with each point of use being able to be identified uniquely and where possibly geographically as well (for mobile resources in the network).
- Network shall have redundant connectivity, paths to acquire data/ signal / voice / video and be able to reach all controllable devices on a real time basis instantly for necessary commands and controls.

Responsibility of MSI

The functional requirements and technical specifications provided in this RFP are indicative and providing guiding rules. The MSI is free to offer products and solutions, which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an Optimized solution, which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved.

Minimum Functional Requirements

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
OFC/FR/1.01	Network Design	• The network design shall at least detail out the network connectivity strategy, network scalability, traffic flow management, bandwidth optimization strategy, security strategy, site-wise bill of material, WAN drawings, Leased Circuit network configuration plan for seamless integration with other infrastructure, etc. Any additional network design aspects, to meet overall scope of work also need to be documented by the MSI. • The network solution shall be based on Leased Circuit platform to manage the traffic flow including but not limited to various applications & services such as Voice, Video & Data. • Further it should provide capability of doing traffic classification and prioritization of applications as per the best practices and requirement of RSCL efficiently.	

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
		• It shall be required to map each location of RSCL's network vis-à-vis the network design and provide technological solution for implementing the network solution at every point of origin of the signal / request into the ICCC and where the device shall be able to support remote commands, the same shall be possible from the ICCC. • It shall be ensured that the network deployed should be IPV4 as well as IPv6 compliant, as also supporting unified communications with all departmental handheld walkie-Talkies, mobile systems, RF and mobile phone communication systems, in addition to enabling Audio, Video communications from end point devices as well as from the ICCC.	
OFC/FR/1.02	Operation, Monitoring, Maintenance and Management of Network services at DC, ICCC and other field locations including the functional upkeep of all deployed devices in the network	• Configuration, Operation, Monitoring, Maintenance and Management of CPE Routers and MUX, Modem installed for the project • Rectifying problems / faults of all Router cores and Switches reporting the status to the RSCL. • Orderly Start-up and Shutdown of all network infrastructure for city network backbone as per the laid down procedures mutually finalized by the RSCL and MSI • Incident wise reporting, Link Availability, Loss of Link Availability, Historical trends for availability should be reported to the RSCL • Daily monitoring of WAN, manual testing, Rectifying and reporting the status to the RSCL. • Maintaining an updated inventory / asset list of complete IT Network Infrastructure • Protocol migration to any protocol as and when required • Configuration / re-configuration / maintenance / monitoring management of Dynamic • Host Configuration Protocol (DHCP) servers installed on core routers, routing tables. • Maintaining and updating IP address list and optimum management of IP addresses through DHCP/Static entry • Maintain and update IP address list and optimum management of IP address • Maintain and update LAN and WAN diagrams with relevant details • Replacement of supplied equipment in case if the hardware is faulty or any parts is non-functioning • Installation, Uninstallation, re-installation of IOS of Routers and Switches due to reasons of bugs, etc. • De-commissioning of the existing network & Establishment of the new Leased Circuits across TSC network in phase manner without disturbing the regular operations & working of the existing software applications • Bandwidth should be managed using tools that ensure availability of bandwidth on a remote basis. The services should ensure that the bandwidth is available to the department as per the requirements • The task of increase or decrease of bandwidth shall be completed as per below requirements: - For planned activities the bandwidth should be augmented before 15 days of date of actual usage, and for unplanned activities selected MSI should augment the bandwidth as per tripartite discussions - Network should also be capable of providing Bandwidth on Demand.	

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
		• Communication Management (NMS proposed under this project to be used for this) - Monitoring of quality of various communication links on LAN, WAN, leased circuit/ISDN and Liaison with ISPs - Link Availability - Alerts for loss of Availability - Historical trends for Availability - Incident-wise Reporting - All incidents leading to downtimes on a particular link should be available at least end-of-day online - Historical trending for today/yesterday/last 7 days/last week/last month should be available • Internet, Intranet and Gateway Access, with internet access being provided to the ICCC, DC and DRC - Daily monitoring of Internet Leased circuits and All Intranet services. - Bandwidth Utilization monitoring and reporting the status to RSCL in case if the utilization on the constant basis is exceeding 80%. - DNS Server and Domain Resolution. - Lookup for Internet hosts. - Proxy Server Configuration, URL filtering and URL Access log. - If any intranet services are not available the status should be immediately reported to RSCL IT Cell.	
OFC/FR/1.03	Reports	• MSI should submit the reports on a regular basis in a mutually decided format. • Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients • The detailed list of reports as well as templates will be decided once the MSI is on-boarded • MSI should also submit certain information as part of periodic review as and when required by the RSCL • Daily Reports - Summary of issues / complaints logged at the Help Desk - Summary of NMS, other performance monitoring tools - Network Bandwidth utilization. - Summary of resolved, unresolved and escalated issues / complaints • Weekly Reports - Issues / Complaints Analysis report for calls, call trend, call history, etc. - Summary of network equipment rebooted. - Summary of issues / complaints logged with the OEMs. - Summary of changes undertaken in the WAN Network including major changes like configuration changes, patch upgrades etc. • Monthly Reports - Component wise physical as well as Network infrastructure availability and resource utilization. - Consolidated SLA / (non)-conformance report - Log of preventive / scheduled maintenance undertaken - Log of break-fix maintenance undertaken - Network Traffic Analysis, pattern identification and suggestions for improvement across network backbone - Network Utilization	

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
		- Network Device Status - Network Uptime Statistics & Threshold violation. - Bandwidth utilization as measured at aggregation point as well as on individual links. • Quarterly Reports - Uptime, Downtime and performance report - SLA compliance Report for the Quarter - Hardware pool Report • Half yearly Reports - Network infrastructure Upgrade / Obsolescence Report. • Incident Reporting - Detection of security vulnerability with the available solutions / workarounds for fixing. • Hacker attacks, Virus attacks, unauthorized access, security threats, etc.	
OFC/FR/1.04	Network Architecture	• All the Leased Circuit coming to its respective office should be terminated as a single Ethernet drop/port and should not be configured with separate Ethernet connectivity from each remote location, at zonal side of connectivity, for each respective ward or remote location. • Leased circuit connectivity should be configured to achieve Multiple Hub & Spoke topology.	
OFC/FR/1.05	Network Design	• The MSI shall be required to integrate the existing LAN (starting from the LAN/Field switch being connected) at each of its locations with the proposed WAN based on Leased Circuits. • Solution designed should have provisions to offer different classes of service in order to prioritize traffic as desired by RSCL without any additional investment. Such service level prioritization will include- packet prioritization, bandwidth prioritization at the application/ source IP/ target IP level. • MSI shall ensure that the network deployed should be IPV4 as well as IPv6 compliant. • The design should also support unified communications with all departmental handheld walkie-Talkies, mobile systems, RF and mobile phone communication systems, in addition to enabling Audio, Video communications from end point devices as well as from the ICCC. • The design should consider supporting network requirement for all the solutions that are in scope of this document.	
OFC/FR/1.06	Redundancy	• Redundancy in connectivity to all remote locations, all connected smart devices, other edge devices, SCADA etc., the ICCC, the DC & between the DC & the DR sites connected through Leased Circuits is essential. Should have redundancy in place to meet necessary SLA requirements.	
OFC/FR/1.07	Network Security	• Security being one of the most important aspects for the RSCL, it would be governed by stringent standards. • There shall not be any network security breach. A breach is said to have occurred if access is denied, an inappropriate access is provided, data theft, malicious postings in any sites, mis-connection or wrong diversion of lawful data to any unauthorized user / portal / unauthorized external storage Security incidents could consist of any of the following: • Denial of Service Attack: - This shall include non-availability of service (Internet bandwidth, messaging service and other web services due attacks that consumes related network resources)	

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
		• Data Theft: - Compromise of any kind of the network. • Intrusion: - Successful Unauthorized access to the RSCL information system, resulting in loss of confidentiality/Integrity/availability of data. • Malicious Traffic: - The MSI shall be responsible for isolation of the node/network in which malicious traffic is generated which may be due to virus, malware etc. on detection. • All active components shall have adequate security provisions, to protect itself from any security attack including but not limited to DoS, password break, malicious software, unauthorized access and recording of all access information in the active components. • Link Security: MSI has to ensure that the link provided is a secure VPN from end to end including CPE, last mile and LAN. • MSI shall be required to bind the MAC address of the computer with IP as and when required by the RSCL. • All the network solution offered by the MSI shall have the security provisions to prevent any unauthorized access to anybody including MSI or its partners. The RSCL may reserve the right to get testing of components/ equipment supplied under this contract by any designated Third Party Agency. • During the currency of the project MSI shall adhere and conform to the Network Security Policy of the RSCL and guidelines issued by Government of India/Government of Odisha from time to time. For all hosted sites and accesses from remote users and citizens, an OWASP or those prescribed by the STQC and CERT-IN guidelines shall have to be cleared before hosting and after any software or hardware system revision / upgrade. • All external points of use / origin of connections and origin of signals shall have to be confirmed periodically by the MSI on a quarterly basis, to be of the same deployed user site and device and is in use by the authorized official user only and any unauthorized use of deployed devices / services on the network shall be directly attributable to the MSI under access breach clauses; due periodic site visit and test reports with authorized user credential inspections shall have to be evidenced by the RSCL.	
OFC/FR/1.08	Operation, Monitoring, Maintenance and Management of Network services at DC, ICCC and other field locations including the functional upkeep of all deployed devices in the network	• Network Performance Monitor - Simplifies detection, diagnosis, & resolution of network issues before outages occur - Tracks response time, availability, & uptime of routers, switches, & other SNMP-enabled devices - Shows performance statistics in real time via dynamic, drillable network maps - Includes dashboards, alerts, reports, & expert guidance on what to monitor & how - Automatically discovers SNMP-enabled network devices & typically deploys in less than an hour - Provides network views in an intuitive graphical format - Discovers network devices and provides a map to illustrate the structure of the network - Provides the status of devices and segments - Help network administrators prevent problems by identifying potential trouble spots before a failure occurs	

S.No	Parameters	Minimum Requirement Specification	Compliant (Yes/ No)
		- Automatically discovers, maps and monitors switches, ports, and network devices - Quickly finds devices and retrieves user name, port details, connection history and more - Enables searching on IP address, user name, Hostname or MAC address to track endpoints - Allows white listing and watch lists with automatic alerts and click-of-a button port shutdown - Provides detailed switch port usage data, capacity analysis, and built-in reporting • Network Configuration Manager - Enables bulk change deployment to thousands of devices - Performs automatic, scheduled network configuration backups - Protects against unauthorized & erroneous network changes - Detects & reports on network compliance policy violations - Provides real-time network inventory & asset service management • Net-Flow Traffic Analyzer - Monitors network bandwidth & traffic patterns down to the interface level - Identifies which users, applications, & protocols are consuming the most bandwidth. - Highlights the IP addresses of top talkers - Monitoring tools include Real-Time Interface Monitor, SNMP real time graph - Diagnostic tools include Ping Sweep, DNS Analyzer, and Trace Route. - Network discovery tools include Port Scanner, Switch Port Mapper, Advanced Subnet Calculator. - Management tools include Real-time Traffic Analyzer, Config Downloader. • IP Address Management Software - Centralizes IP infrastructure management, monitoring, alerting and reporting. - Automatically scans IP address space at customizable, scheduled intervals. - Consolidates multi-vendor DHCP/DNS management via a single, integrated interface. - Delivers real-time, at-a-glance dashboard visibility along with historical tracking. - Provides active IP address conflict detection and preventative alerts. • VOiP Network Quality Manager - Monitors VoIP metrics including jitter, latency, packet loss, and MOS. - Correlates call issues with WAN performance for advanced troubleshooting. - Searches & filters call detail records. - Monitors site-to-site WAN performance.	

Intelligent Waste Management System

Context

With a total of around 69,600 households in the Rourkela Municipal Corporation (RMC) area, the city of Rourkela generates 120 MT[1] per day of solid waste. While there exists 100% door to door waste collection across 15 wards, the remaining 25 wards on an average have only around 35% door to door collection. Nearly 83%[2] of the total solid waste generated in these wards is collected at around 315 identified garbage depots located across the city. Of these garbage depots, only 96 locations have Bins installed for secondary collection of waste with the remaining depots witnessing open dumping of waste. Currently, there are 19 GPS based waste collection vehicles (comprising 1 compactor, 7 tippers, 6 tractors, 2 JCBs, 2 Dumpers, and 1 attacher) deployed for transportation of solid waste from the depots to the land fill site near BPUT. Further, there is no provision for treatment of the solid waste in the city. The entire solid waste management value chain, encompassing primary collection of waste from respective households to the disposal of waste, is managed by Rourkela Municipal Corporation (RMC).

In addition to the solid waste, RMC is also responsible for liquid waste (i.e. Faecal sludge and Septage) management encompassing desludging/ emptying of containment unit (pit, septic tank, etc.), transportation, and its disposal. On an average 5 requests per day[3] is received by RMC from the residents of Rourkela for cleaning of their containment tank. Presently, there are 4 GPS based cesspool vehicles (2 of which are operated by private operator) for cleaning and transportation of faecal sludge to the land fill site near BPUT till the envisaged Septage Treatment Plant becomes operational.

Key issues impeding effective waste management in the city include:

- Absence of any mechanism to monitor lifting of solid waste by the waste collection vehicles from the designated bins
- Absence of tracking of the quantity of waste disposed at the dump yard/ landfill site to ensure transparency in vendor payment towards disposal
- Limited monitoring of the field staff engaged in waste management on a daily basis
- Limited number of compactors resulting in mechanical loading of garbage at only 50% of the community bins

Objective

In order to streamline the overall process of waste management including secondary collection at garbage depots, transportation of waste by waste collection (for solid waste) /cesspool (for liquid waste) vehicles to the landfill /septage treatment plant site, attendance of the field staff, billing and collection, etc. an intelligent waste management system has been proposed to be implemented by the MSI.

Key benefits envisaged from the intelligent waste management system include:

- Real-time tracking of waste collection/cesspool vehicles deployed
- Monitoring of lifting of waste from respective community bins and cleaning of containment units by the vehicles
- Effective billing through generation of demand note for vendor billing as per the weight of the waste disposed on the landfill/septage treatment plant site and collection associated with waste management
- Efficient monitoring of the presence of field staff engaged in waste management activities.
- Logging of complaints/ grievance by the citizens and timely redressal of the same by the concerned officials
- Proper management and monitoring of waste management related activities through analysis of the MIS reports generated, graphical interface along with the mobile application for use by the waste management staff members

[1] RMC officials
[2] RMC officials
[3] RMC officials

Scope of Work

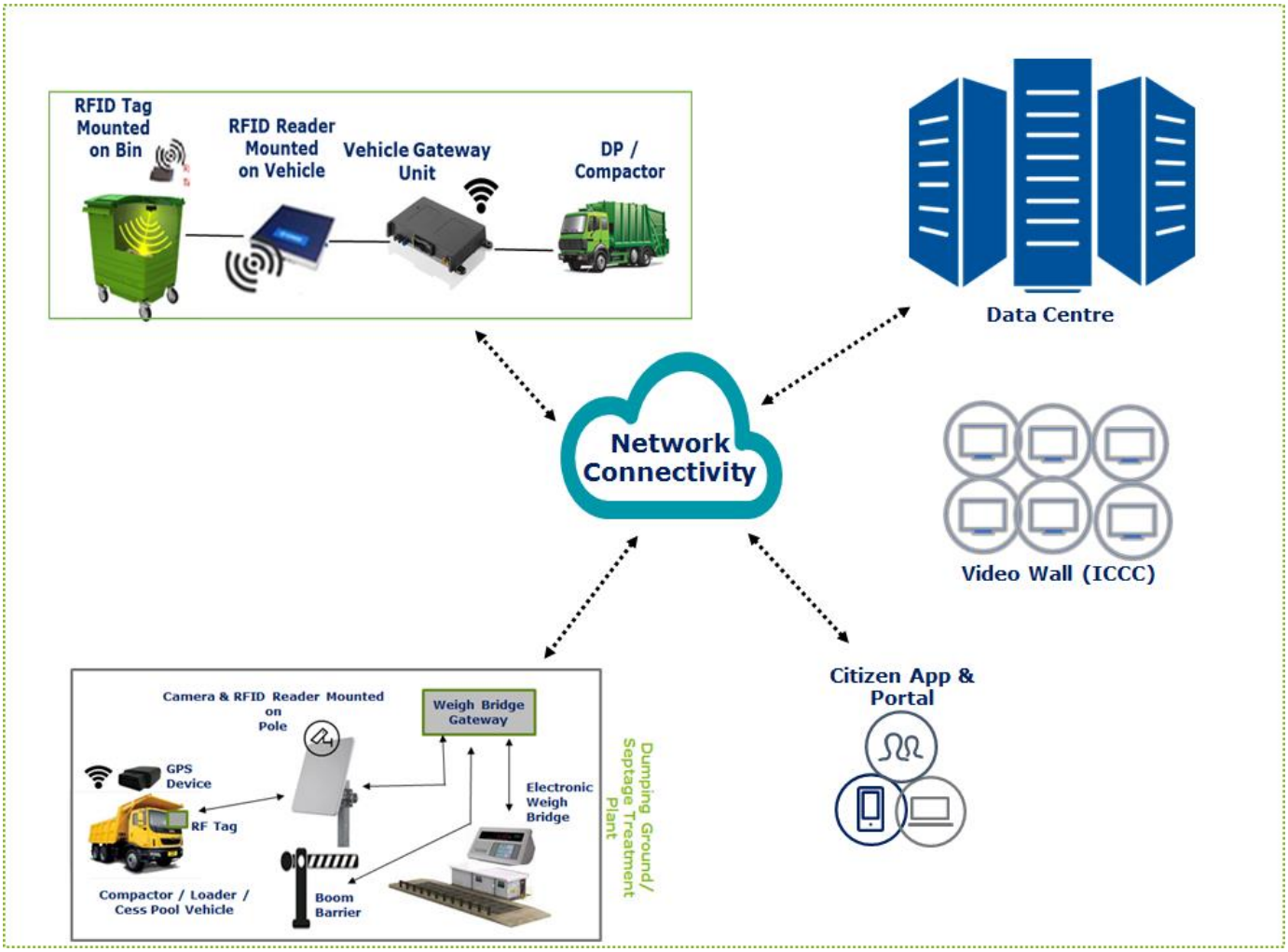
The scope of work for the MSI for implementation of Intelligent Waste Management system shall include but not limited to:

- Installation of RFID devices for waste collection bins at the garbage depots and collection vehicles for bin Tracking and Management
- Installation of RFID devices in cesspool vehicles for their monitoring and management at the disposal/treatment site
- GPS based vehicle tracking and monitoring system devices in waste collection/cesspool vehicles for transit management
- Electronic weighbridges shall be installed to measure the input being carried into by the incoming vehicles to the landfill/septage treatment plant site. The same shall be fed into the weighbridge software for processing data date wise, vehicle wise, etc. The same shall be passed on to ICCC for day-to-day monitoring of waste disposal and for generation of daily, weekly and monthly reports. The MSI shall also have to make a provision for inclusion of any additional weighbridges identified, in the future, to be monitored at the ICCC.
- CCTV surveillance system at the landfill/septage treatment plant site to monitor the waste disposal by waste collection/cesspool vehicles
- Biometric based field Staff Attendance System
- Geocoding / surveying of the Garbage Depots, Vehicle Routes, Landfill site, Septage Treatment Plant and others (as per RSCL/RMC request) shall be done by the MSI. MSI shall use these locations over the maps and shall deliver the same to RSCL/RMC in standard GIS format. The waste management solution should have integration with the GIS map prepared.
- Design, development, supply, and deployment and implementation of web based application software integrated with RFID devices, GPS based collection vehicle devices, weighbridge application, and grievance redressal and monitoring modules.

All the 40 wards of Rourkela Municipal Corporation area, BPUT Landfill and Septage Treatment Plant site comes under the purview of Intelligent Waste Management system.

Indicative Solution Architecture

The diagram below illustrates the key components/ modules of the intelligent waste management system, including solutions related to secondary collection of waste at garbage depots, transportation of waste to landfill site/ septage treatment plant, attendance of the field staff, billing and collection, etc. Please note that the solution architecture is indicative in nature and is given to provide an overview on the overall scope of work and its intended use.



Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. Bin Tracking and Transit Management Module		
IWMS/FR/1.1	Geo tagging of all designated waste bins, septic tanks/containment units located in all the wards by which the latitude and longitude details are reflected in the module pin pointing the location of the Bins, Septic Tanks/Containment Units. All the bins shall be codified with a facility for future scalability.	
IWMS/FR/1.2	System shall be integrated with the RFID system for bin collection management	
IWMS/FR/1.3	Automated Vehicle Location System with a provision for customized dashboard for monitoring and tracking of solid waste collection and cesspool vehicles	
IWMS/FR/1.4	GIS mapping for purpose of highlighting routes covered by the solid waste collection and cesspool vehicles	
IWMS/FR/1.5	Geo fencing of the garbage depots, landfill and septage treatment plant site to facilitate capturing of the GIS information	
IWMS/FR/1.6	Application shall enable the monitoring of transport of Solid/Liquid Waste from Garbage Depots/Households to the Landfill/Septage Treatment Plant site	
IWMS/FR/1.7	RFID reader to be installed on the vehicle to read the RFID tag fitted on the bin (on both sides) when the bin is lifted/ attended. The tag with a unique identification code will help in tracking of respective bins served status.	
IWMS/FR/1.8	Vehicle Gateway unit, mounted on the vehicle dashboard and connected to the RFID reader shall collect and send the data to the waste management application through GSM/ GPRS connectivity to confirm attending of the bin	
IWMS/FR/1.9	Integration with SMS gateway to facilitate notification through SMS on status update of waste pickup from bins and cleaning of containment units/ septic tanks	
IWMS/FR/1.10	Provision for uploading of a picture (taken through phone immediately after unloading the bin and cleaning the surrounding of the bin) of the unloaded waste bin to ensure that the waste from the particular bin has been lifted	
IWMS/FR/1.11	Application shall be hosted in the Integrated Command and Control Centre (ICCC). The application shall leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and provide the same on the dashboard.	
2. Billing and Collection Module		
IWMS/FR/2.1	RFID tagging of waste collection and cesspool vehicles to enable their reading at the entry/exit stations of the landfill/septage treatment plant sites	
IWMS/FR/2.2	Installation of RFID reader and camera on the Pole at entrance/exit of the weigh bridge installed in the dumping ground/septage treatment plant to read the RFID tag on vehicle and capture vehicle details	
IWMS/FR/2.3	Weigh Bridge Gateway to collect data on vehicle details through RFID reader along with the weight details from the installed weigh bridge at the landfill/septage treatment plant site and send the same to the waste management application for generation of demand note for billing purpose. The gateway shall also trigger the boom barrier installed at the landfill site/septage treatment plant to open on completion of weight registration on the application	
IWMS/FR/2.4	All the data shall be stored locally for a minimum period of 60 days including the video and images captured.	
IWMS/FR/2.5	Module shall enable the tracking of vehicles' their inward/outward movement, weight of waste transported to landfill/septage treatment plant site and transfer the same to the ICCC without any ability to change the data locally.	
IWMS/FR/2.6	Integration with payment gateway for online payment of the fees, fines and other kinds of financial transaction as well as integration with POS devices to enable update of onsite payment	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
IWMS/FR/2.7	Provision to accept offline payment by capturing details of Demand Draft/ Bank Challan	
IWMS/FR/2.8	Provision for billing and collection and assessment of the penalty as specified in the Service Level Agreement	
IWMS/FR/2.9	The billing and collection mechanism as well as the assessment of the penalty should be developed in line with the provision of the existing collection and transportation contracts to avoid any conflict in future.	
3. Attendance Module		
IWMS/FR/3.1	GPS based mobile device to enable Authority's/Agencies field staff to register their attendance/presence throughout the day	
IWMS/FR/3.2	Periodic tracking of the location (with time stamping) of the staff through GPS based mobile device and mapping the same with pre-defined area coordinates	
IWMS/FR/3.3	Facility to handle the biographic details of all field level employees (both contractual and on-payroll) along with the provision to capture attendance data daily either on biometric devices or on supervisor certification	
IWMS/FR/3.4	GPRS enabled feeding of data by the device to the ICCC for report generation and alerts	
IWMS/FR/3.5	Integration of attendance data with the HR system of RMC and payroll processing	
4. Service Level Agreement (SLA) Module		
IWMS/FR/4.1	Enable the mapping of the existing Service Level Agreement with all the involved stakeholders for the waste management	
IWMS/FR/4.2	Should map the payment and penalty calculation as specified in the SLA	
IWMS/FR/4.3	Should interact with the other relevant modules to calculate correct remuneration and penalty as per the prevailing contracts.	
IWMS/FR/4.4	Should be configurable to enable the modification of rates of penalty and payment if needed	
5. Grievance Redressal and Monitoring Module		
IWMS/FR/5.1	Facilitate registration of grievances and complaints by the citizens	
IWMS/FR/5.2	Reflect the hierarchy of RMC for escalation of grievances for redressal	
IWMS/FR/5.3	Full redressal workflow management system with auto escalation of grievances as per set time period & escalation hierarchy	
IWMS/FR/5.4	Fully configurable to set up desired levels of escalation hierarchy as well as configure the time period for escalation	
IWMS/FR/5.5	Integration with SMS gateway to enable the notification of status through SMS	
IWMS/FR/5.6	Integration with Simple Mail Transfer Protocol (SMTP) to facilitate notifications to involved stakeholders/ parties through email	
IWMS/FR/5.7	Enable capturing of citizen complaints through call centre as well as through web portal	
IWMS/FR/5.8	Generation of unique compliant ID to enable tracking of complaints/ grievances	
IWMS/FR/5.9	Status update in the web-portal to enable tracking of complaint/ grievance status by the citizens	
IWMS/FR/5.10	Image capture through mobile application for registration of complaints and grievances by concerned citizens	
IWMS/FR/5.11	System should facilitate citizen complaints through SMS and its tracking	
IWMS/FR/5.12	Generation of a system based complaints reports and their status on a daily basis to enable RMC to assess the category of complaints registered and ensure timely redressal of the same	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
6. Waste Management Monitoring Tool		
Web Portal		
IWMS/FR/6.1	To provide information to the citizens with regard to waste management activities as well as generate MIS reports to provide information on various aspects of waste management related activities for better decision making	
IWMS/FR/6.2	Citizen centric web portal to provide all the information related to waste management activities of RMC	
IWMS/FR/6.3	System should show the Graphical view of the statistical data	
IWMS/FR/6.4	Provision for generation of various MIS reports highlighting the waste management related activities undertaken by RMC including: • Daily, weekly, monthly reports on item-wise, dept. wise and activity wise details • Attendance reports • Grievance reports showcasing in-progress, resolved and unattended complaints • Consolidated report generation on garbage depots, containment unit/ septic tank activity • Monitoring the activity and payment to contractors/ workers etc. • Billing and collection reports, etc.	
Web Based GIS		
IWMS/FR/6.5	To provide the graphical interface to monitor the work done by the field staff of waste management activities.	
IWMS/FR/6.6	Web based GIS application denoting all the graphical locations of the bins/garbage depots/ septic tanks/ landfill/septage treatment plant site, etc.	
IWMS/FR/6.7	Collection and Configuration of the geo-locations as per the project requirement	
IWMS/FR/6.8	Designing of the Geo-fencing reporting portal	
IWMS/FR/6.9	GIS system shall be developed with spatial database and integrate with the data captured above for geographic queries and normal data queries.	
IWMS/FR/6.10	Web enabled GIS system with role and responsibility based reporting	
IWMS/FR/6.11	GIS system shall have the required layers such as Zone, Circle, Ward and Locality Garbage Depots, Septic tanks/Containment Units	
IWMS/FR/6.12	GIS based interface to view all the Bin, Septic Tanks/ Containment unit Points at a glance, on location basis and Bin, Septic/ Containment Points locations should be integrated with digital images.	
GPS Tracking		
IWMS/FR/6.13	Movement of all the vehicles will be tracked by a GPS tracker	
IWMS/FR/6.14	The application software shall have facility to read / integrate / capture the GPS data of the vehicle along with generation of different MIS reports	
IWMS/FR/6.15	There shall be a provision of third party application integration / new application software developed for the above purpose	
Mobile Application		
IWMS/FR/6.16	To provide a platform to update on real time basis the status of the activities undertaken by waste management staff along with uploading the graphical evidence of the work done.	
IWMS/FR/6.17	Mobile application in open source platform for each application module proposed under scope of work	
IWMS/FR/6.18	Should include Grievance redressal module and ability to capture and upload image of related complaint or grievance	
IWMS/FR/6.19	Enable supervisors, transporters and other appropriate concerned officials to update the status of their activities	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
IWMS/FR/6.20	Provision to capture the images of the bins, septic tanks/ containment units and transmit the same to the central server with text, image and GPS data such as date and time, latitude and longitude	
IWMS/FR/6.21	Provision for sending notification through SMS when required	
Other Aspects of Application Development		
IWMS/FR/6.22	System shall have built in security for data capturing and transfer including devices used i.e. restricting to the authenticated devices only.	
IWMS/FR/6.23	Encryption techniques if used for data security shall be of minimum 128-bit encryption.	
IWMS/FR/6.24	Uptime of the system shall be maintained at least 98 %.	
IWMS/FR/6.25	Solution shall be operated in production, backup, test and staging environment.	
System Features of IWMS application		
IWMS/FR/6.26	Solution architecture with technology stack shall be clearly defined	
IWMS/FR/6.27	Solution shall be based on open source technology	
IWMS/FR/6.28	Solution recommended shall comply with standards and guidelines of Govt. of Odisha & India.	
IWMS/FR/6.29	Solution shall have role based access and management according to the rules of RMC	
IWMS/FR/6.30	Solution shall have the ability for logging, audit, and tracking of any changes carried out on the database. Only authorized users according to their use rights may make entries to the database	
IWMS/FR/6.31	Declaration of the database software and development tools that is intended to use. Use of any licensed software and the implications for licensing must be fully disclosed.	
IWMS/FR/6.32	Development environment shall be declared for the proposed application software	
IWMS/FR/6.33	Web-based application shall have the capability of being device and browser independent	
IWMS/FR/6.34	Solution shall support N-tier architecture, single-sign on facility and PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA).	
IWMS/FR/6.35	Solution shall maintain Interoperability Standards ensuring that the Software developed is easily integrated with the other Software	
IWMS/FR/6.36	The architecture shall be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance	
IWMS/FR/6.37	The solution shall follow stringent security features such as • The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols. • The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication. • Security design shall provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system. • The solution shall provide for maintaining an audit trail of all the transactions and should also ensure the non- repudiation of audit trail without impacting the overall performance of the system. • The overarching requirement is needed to comply with ISO 27001 standards of security	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
IWMS/FR/6.38	The solution must be compliant with latest versions of Industry Standards such as W3C specifications, Information access/transfer protocols SOAP, HTTP/HTTPS, etc.	
Application Integration		
IWMS/FR/6.39	Application shall be made scalable and robust with ability to be integrated with existing RMC applications or to be developed applications	
IWMS/FR/6.40	Shall be designed and developed in such a manner so as to allow integration with other applications in future if necessary. Application shall be able to integrate with SMS Gateway, Payment Gateway, Handheld PoS Devices, SMTP, RFID Tracking and Boom Barriers	
IWMS/FR/6.41	System shall facilitate transmission of information to RMC/RSCL portal	
SMS Gateway Integration		
IWMS/FR/6.42	To enable transmission of SMS for waste management related tasks	
IWMS/FR/6.43	Co-ordinate to facilitate SMS Gateway	
IWMS/FR/6.44	Configure the Core application with the SMS gateway for sending and receiving SMS	
Operational Support (Onsite & Offsite) and Maintenance		
IWMS/FR/6.45	To ensure proper functioning of the waste management system.	
IWMS/FR/6.46	Onsite support shall be provided in the form of assistance to all field officials / supervisors wherever they face problems in different wards.	
IWMS/FR/6.47	Offsite support shall be provided in the form of maintenance of implemented software	
IWMS/FR/6.48	Submission of regular status reports	
IWMS/FR/6.49	Resolution of all bugs and errors	
IWMS/FR/6.50	Deployment of required technical resources at the RMC office during the operational period as and when it is required along with computer & internet to perform the service without any additional cost such as but not limited to • Functional changes in the application software • System administration • Migration of transactional data • Development of new form / report • Generation of MIS report • Supervision of Project • Any changes in the workflow and core application framework • Any new integration with other system.	
IWMS/FR/6.51	During maintenance phase, upgrades, patches, fixes, security patches and updates of the application software shall be provided	
IWMS/FR/6.52	Comprehensive warranty that covers all components after the issuance of the final acceptance of the application software by RMC	
IWMS/FR/6.53	Responsibility for the day to day operation and maintenance of the application which includes Frontend Modification (if any), Database related queries (Scheduling, backup), maintenance of the Database, and the Customization of report's format (if required) during the contract period	
IWMS/FR/6.54	Onsite Warranty support	
IWMS/FR/6.55	Onsite periodic support for patch management of application and the related database	
Security Audit		
IWMS/FR/6.56	Application security shall be audited by the CERT-IN empanelled Security Agencies.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
IWMS/FR/6.57	All the compliances raised by the Security Agency shall be addressed and the security audited certificate shall be provided before hosting in the data center	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. RFID Readers		
IWMS/TR/1.1	RFID Reader shall have operating frequency range of UHF 865 MHZ to 867 MHZ.	
IWMS/TR/1.2	The RFID reading range of the transceiver antenna mounted on the vehicle at an average height of 3m above the road surface shall be up to 5m.	
IWMS/TR/1.3	RFID Reader antenna type shall be Circularly Polarized.	
IWMS/TR/1.4	RFID Reader shall comply with the protocol: EPC Gen 2, ISO 18000-6C and shall comply with the general conformance requirements of the standard.	
IWMS/TR/1.5	RFID Reader enclosure shall be light weight.	
IWMS/TR/1.6	RFID Reader technology employed should have the capability to optimize read rates for the bin identification application and adapt to instantaneous noise and interference level.	
IWMS/TR/1.7	RFID Reader shall have capability of diagnostic and reporting tools.	
IWMS/TR/1.8	The firmware should be upgradable to support future protocols.	
IWMS/TR/1.9	Reading of Tag & EPC memory for at least 2 tags per second for a moving vehicle with a speed limit of 40 kilometers/ hour.	
2. RFID Tags		
IWMS/TR/2.1	The tag shall be anti-metal, and could be mounted on the metallic surface.	
IWMS/TR/2.2	The tag shall be high temperature resistant and shall be capable of withstanding harsh or challenging conditions.	
IWMS/TR/2.3	The tag shall have long read and write distance.	
IWMS/TR/2.4	The tag shall be durable, reusable.	
IWMS/TR/2.5	The frequency range of the tag shall be between 865~867MHz.	
IWMS/TR/2.6	The tag protocol shall be ISO 18000-6C & EPC CLASS1 GEN2.	
IWMS/TR/2.7	The tag memory configuration shall be EPC: 96bit (H3) and User: 512bit (H3).	
IWMS/TR/2.8	The tag material compatibility shall be metallic and non-metallic substrates.	
IWMS/TR/2.9	The read range (m) on metal surface shall be max. 7.5m for Fixed Reader and max. 3m for handheld reader.	
IWMS/TR/2.10	The Mounting of tag shall be of screw, rivet, superglue, ribbon, double faced adhesive tape type.	
3. GPS Device Unit		
IWMS/TR/3.1	GSM network of 850/900/1800/1900MHz	
IWMS/TR/3.2	GPRS standard of Class 12 TCP/IP	
IWMS/TR/3.3	GPS locating time of 30sec with cold boot (open sky) 5sec with hot boot (open sky)	
IWMS/TR/3.4	GPS Positioning accuracy of 10-15m	
IWMS/TR/3.5	Working temperature as per City requirement	
IWMS/TR/3.6	Working humidity of 5% ~ 95% RH	
IWMS/TR/3.7	GSM quad-band network	
IWMS/TR/3.8	SOS Button	
IWMS/TR/3.9	Two way communication (Hands-free) Button	
IWMS/TR/3.10	Alerts for Tamper and Low Battery	
4. Barrier Gate		

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
IWMS/TR/4.1	The barriers shall be capable of full lane open from a close state in less than 0.9 seconds.	
IWMS/TR/4.2	The housing and any mounting frame shall be fabricated from corrosion- resistant materials.	
IWMS/TR/4.3	It shall be IP 55 rated.	
IWMS/TR/4.4	The barrier shall be driven electrically.	
IWMS/TR/4.5	The barrier motor shall not be damaged when the barrier is blocked in any position	
IWMS/TR/4.6	Exit barriers shall have presence detectors independent system to prevent barrier arms coming down on vehicles while passing.	
IWMS/TR/4.7	Barrier shall be in the form of infrared units and dedicated embedded loops.	
IWMS/TR/4.8	Apart from the barrier arm, the mechanism may not have any moving protrusions that pose a risk to persons standing in close proximity to the barrier.	
IWMS/TR/4.9	The barrier arm shall be fabricated from a light, corrosion resistant material readily and inexpensively available in India.	
IWMS/TR/4.10	The barrier arm shall further have a protective mechanism whereby controlled fracture of the barrier arm occurs without damage to the housing or motor in the event of frontal collision.	
IWMS/TR/4.11	Preference will be given to non-destructive break-away mechanisms. Further, there shall be a protection mechanism to detect the presence of vehicles to avoid accidental hitting on the vehicles, whenever the boom is triggered for closing.	
IWMS/TR/4.12	Suitable power supply scheme shall be implemented by the Bidder to feed the Exit barrier to protect the source from being damaged due to electrical surges / spikes injected by the dynamic (inductive) load.	
IWMS/TR/4.13	Further, the drive shall be so designed as to the damping factor is just sufficient for the drive to operate the booms without any jerks during open / close to avoid freak hitting by the exiting vehicles.	
IWMS/TR/4.14	Barrier arms shall have retro-reflective red stripes in accordance with the local traffic sign standards.	
5. Fixed and PTZ Camera, Lenses and Mounts		
IWMS/TR/5.1	The camera control shall comply with the latest release of Open Network Video Interface Forum (ONVIF) standards.	
IWMS/TR/5.2	The camera shall include an integral receiver/driver. The receiver/driver shall be capable of controlling pan-tilt, zoom and focus locally and remotely from the ICCC.	
IWMS/TR/5.3	The camera shall incorporate AGC circuitry to provide for compensation at low light levels.	
IWMS/TR/5.4	The lens shall be integrated with the camera.	
IWMS/TR/5.5	Video output resolution shall not be less than 1920x1080 pixels.	
IWMS/TR/5.6	The camera shall be capable to produce minimum 30 frames per second (fps).	
IWMS/TR/5.7	The camera shall provide automatic white balance, automatic exposure, automatic gain control, electronic shutter, and backlight compensation.	
IWMS/TR/5.8	The camera shall be a true day/night cameras with mechanical IR cut filter.	
IWMS/TR/5.9	The camera shall be capable of providing a high contrast colour picture with a full video output at a minimum illumination as mentioned in the specifications.	
IWMS/TR/5.10	All cameras shall capture high definition video, compress the video using H.264, H.265 technique and transmit real-time using fibre optic based communications system.	
IWMS/TR/5.11	The cameras shall capture audio and compress using G.711 technique and transmit real-time using fibre optic based communications system.	
IWMS/TR/5.12	All cameras shall support on-board real-time video content analysis.	
IWMS/TR/5.13	All cameras shall support both Constant Bit-Rate (CBR) and Variable Bit- Rate (VBR) options.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
IWMS/TR/5.14	The camera shall support up to 2 video profiles, each providing independent configuration of bitrate, framerate and resolution.	
IWMS/TR/5.15	The camera shall support video compression up to 6Mbps.	
IWMS/TR/5.16	The camera shall support audio compression using the G.711 compression	
IWMS/TR/5.17	The camera shall support on-board storage via micro SDHC slot and card with a minimum capacity of 64 GB.	
IWMS/TR/5.18	All cameras shall have integral in-built or external adaptive IR technology. For fixed cameras, the IR shall support a range of at least 30m and for PTZ it shall support a range of at least 200m moving with zoom (adaptive).	
IWMS/TR/5.19	For Fixed Cameras: • The fixed camera shall provide a minimum focal length range of 3- 10 mm compensated with digital zoom and shall be remotely controllable from the camera control transmitter at ICCC. • The fixed camera shall capture video using 1/3" progressive scan CMOS or better. • Fixed Camera resolution shall be 1920 x 1080 or better.	
IWMS/TR/5.20	For PTZ Cameras: • Camera shall have capabilities of PAN of 360° continuous. • Camera shall have capabilities of Tilt of 180°. • Lens of 6mm-129mm with minimum 20X optical and 12X digital zoom. • PTZ camera shall capture video using minimum 1/3" type CMOS sensor or better. • It shall support resolution of 1920x1080 or better. • Camera shall support tilt of 100° either side. The tilt capability shall include both the horizontal (level view) and vertical (downward view) position. If the camera travels beyond straight down, automatic image flip circuitry shall prevent the display of an inverted image. • The pan and tilt mechanism shall be an integral part of the camera. • Pan speed shall be upto 160°/s and Tilt speed upto 120°/s.	
IWMS/TR/5.21	There shall be a minimum of 100 assignable automatic preset positions.	
IWMS/TR/5.22	There shall be a minimum of 8 definable privacy zones.	
IWMS/TR/5.23	All cameras shall provide effective 24/7 imaging performance for CCTV surveillance applications.	
IWMS/TR/5.24	All cameras shall provide user control, with remote configuration for functions including streaming and compression settings, exposure, white balance, flicker control, picture size, cropping/privacy, brightness, sharpness, saturation, day-night switching point, frame rate, image rotation, snapshot, dynamic bandwidth allocation and motion detection.	
6. Static Weigh Bridge		
IWMS/TR/6.1	Digital road weighbridge model number as per weights and measures department, confirming to BIS 9281 standards based upon 8 load cells resting on I beam section and MS Plates platform size of 18 m x 3m 120 Tonnes.	
IWMS/TR/6.2	Modular made of RS joists bolted with expansion joints as per BIS 2062 SAIL / TATA.	
IWMS/TR/6.3	Top deck Plates of Mild steel as per BIS 2062 SAIL.	
IWMS/TR/6.4	Load cells of Rocker Column type stainless steel with self-aligning principle.	
IWMS/TR/6.5	Load cells Mounting of MS galvanized with built in pad plates.	
IWMS/TR/6.6	Digital Weight Indicator of stainless steel housing with front panel calibration in accordance to W&M department and Model approval.	
IWMS/TR/6.7	Junction Box of stainless steel IP 65 built in surge protection.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
IWMS/TR/6.8	Outdoor display Board Stainless steel with LED for viewing in all- weather condition.	
IWMS/TR/6.9	The printer shall be Laser Jet Printer. Print speed shall be 30ppm minimum (letter) with resolution of 600 by 600 dpi or better with Resolution Enhanced Technology. The printer processor shall be 266 MHz with memory of 16 MB. The printer shall have at least one Hi-speed USB 2.0 port	
IWMS/TR/6.10	Weight management and picture capture with GVW, DTM stamp, direction, material, source destination.	
IWMS/TR/6.11	It shall have the capability to work as standalone as well integrated system.	
IWMS/TR/6.12	The platform shall comprise of medium beams sections of SAIL/TATA as per BIS 2062 with 100% overloading capacity. Platform design would be universal i.e. the weighbridge can be used in Both Pit / Pit less type application. Furnishing 2 Epoxy coats to prevent any rusting, external weather conditions.	
IWMS/TR/6.13	Structure which can be fully expandable & relocatable and be used for a Pit or Pit less type foundation in case of relocations in the future. The Structure should have approval from any recognized institution IIT / NPL / designed as per Staad – III. Approx. Structural Weight – 11 Tonnes.	

Intelligent Traffic Management System

Context

Rourkela Municipal Corporation (RMC) is spread over an area of around 53.3 sq.km and is covered with around 658[4] kms of road network, comprising a total of 44 traffic junctions[5] or intersections, as depicted in the map below. These traffic junctions can be broadly categorized into three types namely, (i) Three arm junctions (26 nos.), (ii) Four arm junctions (17 nos.) and (iii) Six arm junction (1 no.). Currently, only three junctions namely, Chhend Chowk, 7/17 Chowk and Indira Gandhi Park Chowk have traffic signals installed. Out of these, only one junction at Indira Gandhi Park Chowk has an operational signal, while the other junctions are being managed manually by traffic police.

Further, as per vehicle registration data obtained from the RTO office of Rourkela, number of registered vehicles have increased at a CAGR of 15% during FY 2014-17 contributing to significant increase in road traffic

Key issues observed in terms of traffic management across the city are as follows:

- Absence of traffic signals results in (a) traffic congestion in peak hours, (b) higher incidence of accidents and (c) unsafe pedestrian movement
- Limited functionality for incident management system with regard to creating green corridors for emergency (ambulance, police, etc.) vehicles
- Absence of any facilities like pelican signs or blinkers at the traffic junctions for providing assistance to the pedestrians while crossing the road.
- Absence of any automated traffic monitoring system across intersections resulting in undetected traffic violation and increase in traffic accidents.
- Lack of a proper demarcation of no entry zones or one-way road adversely impacting the traffic movement and resulting in higher traffic violations
- Prevalence of manual issues of challan with limited evidence in the form of visual proof against the traffic violators

Intelligent Traffic management system comprises key components/ modules viz. (a) Adaptive Traffic Signal Control System (ATCS) and (b) Traffic Violation Detection System (TVDS). The sections below highlight the overall project objective and key benefits envisaged form the proposed solution for the respective components/ modules.

Adaptive Traffic Signal Control System

Objective

ATCS is a traffic responsive system which uses real-time data on vehicular traffic to optimize traffic signal settings and reduce vehicle delays, queue length of vehicles at the junctions/ intersections in order to enhance capacity and efficiency of the road network.

Key benefits envisaged from installation of ATCS include:

- Reduce vehicular delays and related greenhouse gas emissions
- Improve operational planning, efficiency and capacity of road network
- Improve Incident Management System by creating green corridors through pre-emption and priority for emergency and special vehicles

Scope of Work

The broad scope of work to be covered under ATCS sub module shall include the following, but is not limited to:

- Preparation of Solution Architecture as per project blueprint to develop a final BOQ for installation traffic signalling systems.

[4] City Development Plan of Rourkela
[5] RTO, Rourkela

- Integration of ATCS field infrastructures with the proposed ATCS software application
- Configuration of traffic signal at each of the junction along with development of signal control plan for individual operations, coordinated signal plan for the junction in sync with the area wide signal plan for different operating conditions. The operating conditions may include different peak and off-peak conditions, special events, contingency plans etc.
- The MSI should design and propose energy saving signalling system by using solar powered signals or other advanced technologies.

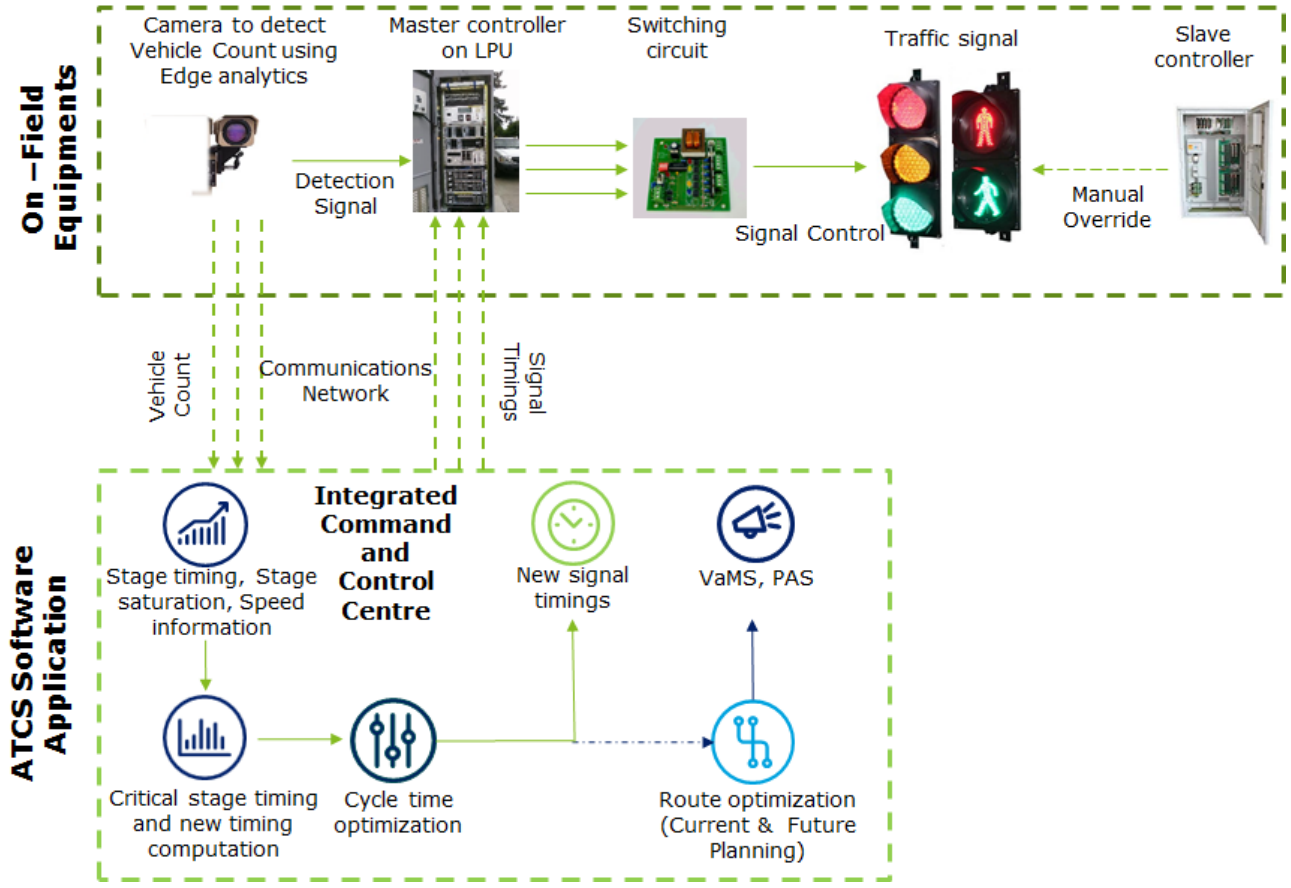
Installation of vehicle detectors, controllers, Traffic light aspects, poles, cantilevers, junction Box and other required accessories at 29 traffic junctions are given in the table below for successful operation of the ATCS for RSCL and Rourkela Traffic Police

S.No.	Junction Name	Type of Junction (No. of Arms)
1	Birsa Chowk	6
2	Traffic tower	3
3	Sector-2	4
4	Ambagan Chowk	4
5	7/17 Chowk	4
6	7/15 Chowk	4
7	Sector-8	4
8	DPS Chowk	4
9	Air strip Chowk	3
10	SOS Village Chowk	3
11	Chhend Chowk	3
12	DAV Chowk	4
13	Gadiatola Chowk	4
14	Municipality Chowk	3
15	Sarna Chowk	3
16	Bania Chowk	4
17	Traffic gate	4
18	Madhusudan Chowk	4
19	Hockey Chowk	3
20	Panposh Chowk	4
21	Shani Mandir	3
22	Hi-tech Medical Chowk	3
23	Civil Township parking Chowk	3
24	Dandiapadi Chowk	3
25	Vedvyas Chowk	3
26	Rangila Chowk	4
27	Chhend BSNL Chowk	4

S.No.	Junction Name	Type of Junction (No. of Arms)
28	Diesel Colony Chowk	3
29	Chowdhary Petrol Pump	3

Indicative Solution Architecture

The sections below highlight the key elements proposed in the smart solution and overall the process flow and high level functionality of each hardware and software elements of the solution. The high level schematic diagram of the proposed solution architecture for the ATCS project is presented below.



ATCS system comprises of on street hardware component such as camera based vehicle detector which detects the presence of vehicle approaching and waiting at the junction. This information is send to the command centre via master controller system. Here the data is analysed through the ATCS application which process the data and calculates the optimum time phase for maximizing the green phase for each direction and send the information back to the master signal controller which activates the traffic signal as per the optimized time period. Apart from the Master controller at each junction there are slave controller at each of the arms of the signal poles from where the traffic personnel at the junction can change the phase timings of the signal as per requirement for priority green channel as per need.

The solution architecture shall support scalability, open standards, ensure availability, security, interoperability, universal access IT systems, single-sign on, support for PKI-based authentication and authorization, GIS integration etc.

Industry standard best practices shall be carried out to achieve high level stability and robustness of the application. The standards shall at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time)

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. Traffic Signal Controller		
ATCS/FR/1.1	The Traffic signal controller shall be capable of functioning under different modes of operation based on vehicular traffic including Fixed Time, Vehicle Actuation with all stages pre-emption, vehicle actuation with fixed cycle time, and full ATC mode of operation.	
ATCS/FR/1.2	The Controller shall be adaptive in order to be controlled through the central traffic control centre at an individual junction or as part of group of traffic junctions along a corridor or a region.	
ATCS/FR/1.3	The controller shall have the facility to update the real time clock (RTC) from adaptive traffic control system (ATCS) server, global positioning system (GPS) and through manual entry.	
ATCS/FR/1.4	The controller shall be capable of communicating with the ATCS server through ethernet on a managed leased line network or any other appropriate stable communication network.	
ATCS/FR/1.5	The controller shall have a conflict monitoring facility to ensure that conflicts are pre-flagged at the programming stage and these are disallowed even during manual override phase.	
ATCS/FR/1.6	The controller shall provide a dedicated panel with provision for lock and key arrangements for use by the Traffic Police.	
ATCS/FR/1.7	Fixed Time: In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no pre-emption shall be made on any stage. Cycle time remains constant in every cycle execution for a given time period.	
ATCS/FR/1.8	Vehicle Actuation with All Stages Pre-emption: In the vehicle actuation with all stages pre-emption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.	
ATCS/FR/1.9	Semi-Actuation: In the semi-actuation mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.	
ATCS/FR/1.10	Stage Skipping: The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till clearance amber time of the previous stage.	
ATCS/FR/1.11	Vehicle Actuation with Fixed Cycle length: In vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time shall be maintained constant during a given timeslot. Pre-emption for all demand actuated stages except for Priority Stage shall be possible.	
ATCS/FR/1.12	Full adaptive traffic control system (FATCS): In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage and Cycle time specified by the Central Computer during every cycle switching. Pre-emption for	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified time period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. Fall back mode of the traffic signal controller shall be vehicle actuated. On restoration of the communication with central computer the traffic signal controller shall automatically resort to FATCS mode.	
ATCS/FR/1.13	The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at ICCC. - Hurry Call - Flashing Amber / Flashing Red - Junction Off	
ATCS/FR/1.14	If not reverted to the normal operation within the time period listed below, the traffic signal controllers shall timeout the commands and operate normally - Hurry Call – 5 Minutes - Flashing Amber / Flashing Red – 30 Minutes - Junction Off – 30 Minutes	
ATCS/FR/1.15	The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate.	
ATCS/FR/1.16	Green time actually exercised for each approach (stage pre-emption timing) against the Green running period set for the approach by the Central Computer	
ATCS/FR/1.17	Phases - The controller shall have facility to configure Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.	
ATCS/FR/1.18	It shall be possible to operate the filter green (turning right signal) along with a vehicular phase. The filter green signal shall flash for a time period equal to the clearance amber period at timeout when operated with a vehicular phase.	
ATCS/FR/1.19	The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.	
ATCS/FR/1.20	It shall be possible to configure any phase to the given lamp numbers at the site.	
ATCS/FR/1.21	Stages – The controller shall have facility to configure Stages	
ATCS/FR/1.22	Cycle Plans – The controller shall have facility to configure Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in fixed mode of operation.	
ATCS/FR/1.23	Day Plans – The controller shall have facility to configure each day of the week with different day plans. It shall also be possible to set any of the day plans to any day of the week. The controller shall have the capability to configure 20 day plans.	
ATCS/FR/1.24	Special Day Plans- The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.	
ATCS/FR/1.25	Starting Amber - During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for a time period of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. Facility shall be available to configure the time period of Starting Amber within the given limits at the site.	
ATCS/FR/1.26	Inter-green- Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter-green period from 3 Seconds to 10 Seconds.	
ATCS/FR/1.27	Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. It should not be possible to pre-empt the Minimum Green once the stage start	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	commencing execution.	
ATCS/FR/1.28	All Red – Immediately after the Starting Amber all the approaches should be given red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.	
ATCS/FR/1.29	Signal lamps monitoring -The controller shall have inbuilt circuitry to monitor the lamp status	
ATCS/FR/1.30	Green - Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or short circuit in the output) shall force the signal into Flashing Amber / Flashing Red.	
ATCS/FR/1.31	Cable less Synchronization - It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without communication network. GPS enabled RTC shall be the reference for the cable less synchronization.	
ATCS/FR/1.32	Lamp Switching: The controller shall have maximum 64 individual output for signal lamp switching, configurable from 16 to 32 lamps. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating	
ATCS/FR/1.33	Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of vehicle.	
ATCS/FR/1.34	Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server	
ATCS/FR/1.35	Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.	
ATCS/FR/1.36	Real-time Clock (RTC): The GPS receiver for updating time, date and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.	
ATCS/FR/1.37	The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.	
ATCS/FR/1.38	Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).	
ATCS/FR/1.39	It shall be possible to set the RTC from the Central Server when networked	
ATCS/FR/1.40	Keypad (optional): The traffic signal controller shall have a custom made keypad or should have provision for plan upload and download using PC/laptop/Central Server	
ATCS/FR/1.41	Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.	
ATCS/FR/1.42	Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A pre-emption input may be used to demand the Hurry Call mode to give right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements.	
ATCS/FR/1.43	One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red.	
ATCS/FR/1.44	One Auto / Manual Switch: Activation of this switch should enable manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption.	
ATCS/FR/1.45	One Manual Advance Pushbutton Switch: In manual operation mode, the stages	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances.	
ATCS/FR/1.46	One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch the traffic signal controller shall resume its normal operation without violating any safety clearances.	
2. Camera based Vehicle Detector		
ATCS/FR/2.1	The detector equipment shall be a separate logic unit, which may be integrated with the controller, or alternatively mounted in its own housing. The outputs of the detectors indicate the presence of vehicles and are used to influence the operation of the traffic signal controller and shall generate counts, demands and extensions for right-of-way. Means shall be provided so that a detector may be connected to demand and / or extend a phase movement as specified. The detector shall be able to count vehicles in a non-lane based mixed traffic flow conditions with the accuracy being significantly high (over 90%) under all light and weather conditions.	
ATCS/FR/2.2	A detector that does not change its status at least once during a stage execution shall be notified to the Central Computer (in ATCS mode) at the termination of the associated stage.	
ATCS/FR/2.3	Communication Network-The communication network shall enable remote monitoring and management of the intersection and provide for transmission of real-time data (i.e. RTC time, stage timing, mode, events, etc.) from the traffic signal controller to the central computer in Traffic Command Centre (TCC).	
ATCS/FR/2.4	The central computer running the ATCS application shall send optimum signal timings to all intersections in the corridor leveraging the communication network.	
3. ATCS Software Application		
ATCS/FR/3.1	The ATCS shall operate in real time with the capacity to calculate the optimal cycle times, effective green time ratios, and change intervals for all system traffic control signal controllers connected to it. These calculations shall be based on assessments carried out by ATCS application software, running on the Central computer based on data gathered by vehicle detectors. Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.	
ATCS/FR/3.2	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersection in that corridor or region.	
ATCS/FR/3.3	Stage optimization to the best level of service shall be carried out based on the traffic demand.	
ATCS/FR/3.4	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.	
ATCS/FR/3.5	Offset correction shall be carried out to minimize number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.	
ATCS/FR/3.6	The system shall have provision to configure priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.	
ATCS/FR/3.7	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand.	
ATCS/FR/3.8	Propose timing plans to every intersection under the ATCS in every Cycle.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
ATCS/FR/3.9	Verify the effectiveness of the proposed timing plans in every cycle.	
ATCS/FR/3.10	Identify Priority routes.	
ATCS/FR/3.11	Synchronize traffic in the Priority routes.	
ATCS/FR/3.12	Manage and maintain communication with traffic signal controllers under ATCS	
ATCS/FR/3.13	Maintain database for time plan execution and system performance.	
ATCS/FR/3.14	Maintain error logs and system logs.	
ATCS/FR/3.15	Generate Reports on request.	
ATCS/FR/3.16	Graphically present signal plan execution and traffic flow at the intersection on desktop.	
ATCS/FR/3.17	Graphically present time-space diagram for selected corridors on desktop.	
ATCS/FR/3.18	Graphically present network status on desktop.	
ATCS/FR/3.19	Make available the network status and report viewing on Web.	
ATCS/FR/3.20	The ATCS shall generate standard and custom reports for planning and analysis.	
ATCS/FR/3.21	It shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post implementation analysis and study of the proposed ATCS control strategy.	
ATCS/FR/3.22	Shall have ability to predict, forecast and smartly manage the traffic pattern across the signals over the next few minutes, hours or 3-5 days and just in the current real time.	
ATCS/FR/3.23	Shall provide a decision support tool for assessing strategies to minimize congestion, delays and emergency response time to events via simulation and planning tools linked with real time traffic data and control of traffic signaling infrastructure on ground.	
ATCS/FR/3.24	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kinds (traffic states, signal states, vehicle trajectories, incidents, road works, etc.)	
ATCS/FR/3.25	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from abovementioned observations, including vehicle trajectories, through a number of map matching, data validation, harmonization and fusion processes.	
ATCS/FR/3.26	Shall extend the measurements made on only a number of elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future.	
ATCS/FR/3.27	Shall forecast the traffic state with respect to current incidents and traffic management strategies (e.g. traffic signal control or variable message signs), improving the decision making capabilities of the operators even before problems occur.	
ATCS/FR/3.28	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess results.	
ATCS/FR/3.29	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control.	
ATCS/FR/3.30	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops in flow, up to total queue lengths along emission sensitive roads surpassing a definable threshold).	
ATCS/FR/3.31	Shall distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a “traffic data and information hub”	
ATCS/FR/3.32	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
ATCS/FR/3.33	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times based on the data collected continuously over time.	
ATCS/FR/3.34	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network.	
ATCS/FR/3.35	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller	
ATCS/FR/3.36	System shall generate Corridor based and Intersection based reports. The application software shall generate the following reports, but not limited to the below.	
ATCS/FR/3.37	All the reports shall be possible for selected dates.	
ATCS/FR/3.38	Stage Timing report – The report shall give details of time at which every stage change has taken place. The report shall show the stage sequence, stage timings and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage pre-emption time).	
ATCS/FR/3.39	Cycle Timing report – The report shall give details of time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day.	
ATCS/FR/3.40	Stage switching report – The report shall give details of time at which a stage switching has taken place. The report shall show the stage sequence, stage timings and stage saturation for a day.	
ATCS/FR/3.41	Cycle Time switching report – The report shall give details of time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.	
ATCS/FR/3.42	Mode switching report – The report shall give details of the mode switching taken place on a day.	
ATCS/FR/3.43	Event Report - The report shall show events generated by the controller with date and time of event.	
ATCS/FR/3.44	Power on & down: The report shall show time when the master is switched on, and last working time of the master controller.	
ATCS/FR/3.45	Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through keypad or automatically by light-dependent resistor (LDR) with time stamp.	
ATCS/FR/3.46	Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server.	
ATCS/FR/3.47	RTC Failure – The report shall show the time when RTC battery level goes below the threshold value.	
ATCS/FR/3.48	Time Update – The report shall show the time when the Master controller updated its time either manually through keypad, automatically by GPS or through remote server.	
ATCS/FR/3.49	Mode Change – The report shall show the time when Master controller's operating mode is changed either manually through keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL.	
ATCS/FR/3.50	Lamp Status Report – The report shall show lamp failure report with date and time of failure, colour of the lamp and associated phase	
ATCS/FR/3.51	Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.	
ATCS/FR/3.52	Conflict – The report shall show the conflict between lamps (RED, AMBER,	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	GREEN) in the same phase or conflict between lamps with other phase.	
ATCS/FR/3.53	Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day	
ATCS/FR/3.54	Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation and degree of saturation of all the intersections in a corridor for every cycle for a day	
ATCS/FR/3.55	User login – Operator authentication shall be verified at this screen with login name and password	
ATCS/FR/3.56	Network Status Display – This online display shall indicate with appropriate colour coding on site map whether an intersection under the ATCS is online or off. On double clicking the intersection a link shall be activated for the traffic flow display for the intersection.	
ATCS/FR/3.57	Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed and elapsed stage time.	
ATCS/FR/3.58	Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.	
ATCS/FR/3.59	Reports Printing / Viewing – This link shall allow selection, viewing and printing of different reports available under ATCS	
ATCS/FR/3.60	Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.	
ATCS/FR/3.61	Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.	
ATCS/FR/3.62	Junction names shall be identified with each plot.	
ATCS/FR/3.63	Facility shall be available to plot the time-space diagram from history.	
ATCS/FR/3.64	Currently running stage and completed stages shall be identified with different colours.	
ATCS/FR/3.65	Stages identified for synchronization shall be shown in a different colour.	
ATCS/FR/3.66	Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions.	
ATCS/FR/3.67	It should be possible to freeze and resume online plotting of Time-Space diagram.	
ATCS/FR/3.68	The system shall have other graphical interfaces for configuring the ATCS, as appropriate.	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. Fully Adaptive Electric & Solar Powered Wireless Vehicle Actuated Traffic Signals		
ATCS/TR/1.1	Traffic Signals designed for working in wireless/wired medium using WiTrac Master & Slave Controller for running the signal. If wired connection is provided, the wiring shall be done using trenchless technology	
ATCS/TR/1.2	The controllers shall be powered through solar power with 72 hours power backup.	
2. Master Controller- Microprocessor Based Wireless Controller		
ATCS/TR/2.1	The Master Controller shall be a vehicle actuated road traffic Signal Controller, capable of operating the Slave Controllers and Signal lights over wireless medium having Inbuilt GPS module for time synchronization, USB port and RS232 debug port for status monitoring.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
ATCS/TR/2.2	Master Controller shall provide: - 8 input Sensing for Vehicle detection (Universal Vehicle detectors – Inductive or Virtual Loop Camera based), - 16 optically isolated solid state lamp driving output, Capable to command 15 Slaves Controller, - Working Voltage - 12 V DC - Solar Power Compatible, - Power Consumption - 3.6 Watts, - Should have CAN port for wired connectivity to slave controller, - Controller to be fully Adaptive with Necessary communication port to be linked with Control room software to work as Intelligent – Real Time Full Adaptive centrally controlled + Coordinated Traffic Signal controller, - The Local controller will be housed in Pole mounting Cabinet Rain and Dust Proof complete in all respect.	
ATCS/TR/2.3	Other features of Master Controller shall include: - 64 bit microcontroller based Processor (CPU) - Distributed architecture - 1 Master and Slave controller (scalable from 1 to 15) - Signal Switching and feedback on wireless medium - Operate in unlicensed 2.4 GHz ISM Band - Optimized Solar Power - 12V DC operation - Pole mountable Master and Slave controllers - Power efficient LED signal aspects - External Memory: EEPROM (1MB) - Design: Modular & Scalable - CPU: 32 bit microcontroller - Memory: Internal Memory: Flash (512K), RAM (128K)	
ATCS/TR/2.4	Real Time Clock Selection shall be through: - Calendar Clock (RTC) with 10 years Battery back-up. Clock accuracy better than +/- 1 minute per month - Inbuilt GPS Module for time synchronization with Accuracy +/-1 sec. per year - Facility to update from ATCS server, GPS and through manual entry	
ATCS/TR/2.5	Controller shall allow auto shut down on power fluctuation beyond limit & Auto Start up on restoration.	
ATCS/TR/2.6	Controller shall provide through solid state devices, 16 outputs per Master and Slave controller (scalable from 32 to 256 outputs).	
ATCS/TR/2.7	The police control panel on the Controller shall support switches for Lamp OFF, Flash, Auto/Manual, Manual Advance & 4 Hurry Calls.	

ATCS/TR/2.8	Master Controller shall provide:
	- ATCS Interface: 10/100Mbps RJ45 Ethernet port
	- Programming Facility
	  ▪ Built In Keyboard & LCD Display
	  ▪ Laptop Software
	- Firmware Update: Through USB/RS232
	- Status Monitoring and Data Logging: RS 232/Ethernet
	- Auxiliary I/O Interface: 8 Auxiliary I/O Interface
	- Output Protection: Open circuit, Short circuit, over load
	- Input/output Isolation: Optical Isolation.
	- Signal Plan Configuration	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)

	- Built-in Keypad Facia with backlit LCD Display.
	  ▪ Plan download and upload through local Laptop
	  ▪ Plan download and upload through remote Laptop
	- Vehicle / Pedestrian Demand Actuation: Scalable from 20 to 76 inputs in any Combination
	- Time Resolution: 100 millisecond
	- ATC Compatibility: CoSiCoSt and NTCIP or equivalent protocols before System Acceptance.	

ATCS/TR/2.9	Additional Special Features of Master Controller shall include: - The cabinet should have provision to install video detection card for vehicle detection and controller must have feature to integrate with red light violation at later stage. - Cabinet must have space for mounting integration card for RFID/ GPS based Vehicle prioritization at a later stage - Cabinet must have space for intersection with ITS equipment (5 CCTV cameras, red-light enforcement, etc.) components that shall be placed in the same cabinet. - Technology shall be upgraded time to time free of cost during the duration of the Contract.	
3. Slave Controller		
ATCS/TR/3.1	Wireless Slave Controller shall operate on command of Master Controller with 16 optically isolated solid state lamp driving outputs, 4 optically isolated Vehicle detector interface supports inductive loop, Camera and microwave based vehicle detection.	
ATCS/TR/3.2	It shall provide USB Interface - Firmware update, CAN interface; and provide Signal Switching (optional) with RS232 debug port for status monitoring and data logging (Working Voltage - 12 V DC - Solar Power Compatible)	
4. Traffic Signal Heads		
ATCS/TR/4.1	The signal heads shall be as per the low power consumption for all colors	
ATCS/TR/4.2	300mm Hi Flux RED LED aspect 12 V or 24 V DC with inbuilt voltage / current regulator 400 mA Max. including dust and water proof Polycarbonate housing and clamps	
ATCS/TR/4.3	300mm Hi Flux AMBER LED aspect 12 V or 24V DC with inbuilt voltage / current regulator 400mA Max. including dust and water proof Polycarbonate housing and clamps.	
ATCS/TR/4.4	300mm Hi Flux GREEN ARROW LED aspect 12 V or 24V DC with inbuilt voltage / current regulator 200 mA Max. including dust and water proof Polycarbonate housing and clamps.	
ATCS/TR/4.5	300mm Hi Brite with diffusions PEDESTRIAN LED aspect - 2 in 1 Pedestrian Red Man standing and Pedestrian Green man walking with Multi color Display for pedestrian timing. In Metal body of 320 mm x 320 mm minimum display area.	
ATCS/TR/4.6	Drill holes needed for the installation of traffic signal heads shall be further protected by a rubber grommet.	
ATCS/TR/4.7	All the wiring shall be colour coded according to local Indian electrical codes.	
ATCS/TR/4.8	Conductors within poles, pulling boxes or traffic signal cabinets shall be neatly arranged and shall be cabled together with self-clinching nylon cable ties or other method approved by the owner's engineer.	
ATCS/TR/4.9	Traffic signal heads shall be plumb and securely attached with all fittings so they present a neat appearance. All traffic signal heads shall hang at the same elevation.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
ATCS/TR/4.10	All signal heads shall be covered with burlap bag or opaque plastic/vinyl bags while mounted and not in operation. Inoperative signals on roads open to the public shall always be covered. Tilting the signals upward is not an acceptable alternative to covering the heads.	
5. Traffic Signal Cabinet and Equipment		
ATCS/TR/5.1	The Master controller cabinet is to be installed at the place indicated on the traffic signal design drawing approved by the client.	
ATCS/TR/5.2	All schematic wiring diagrams of the Master & Slave controller units and auxiliary equipment, all cabinet diagrams and all operation manuals shall be submitted at the time the controller assemblies are delivered. The diagrams shall show in detail all circuits and parts.	
ATCS/TR/5.3	Conductors within the traffic signal cabinets shall be neatly arranged and shall be cabled together with self-clinching nylon cable ties, or other similar equal method.	
ATCS/TR/5.4	The cabinet shall be IP protected with a rating of IP 65.	
ATCS/TR/5.5	The cabinet shall be MS powder coated enclosure.	
ATCS/TR/5.6	Traffic Signal Controller Cabinets shall have space to accommodate traffic signal hardware and other intersection based Pan City proposal needs (such as hardware for red-light enforcement, surveillance cameras, switches, emergency pre-emption equipment, etc.).	
6. Transit Signal Priority (TSP) System		
ATCS/TR/6.1	The controller shall be capable of supporting TSP at a later stage.	
ATCS/TR/6.2	It is expected that part of TSP roadside components will be installed at the traffic signal cabinet. The proposed traffic signal cabinet shall have enough room to allocate TSP components.	
ATCS/TR/6.3	LED Light Should be designed that Failure of one LED should not result Loss of more than 5% of pixels (Input Voltage: 12 Volts DC)	
ATCS/TR/6.4	Protection system: Fire Retardant, Glass Epoxy, FR4 Printed Circuit Board with protective cover and plain Polycarbonate Lens.	
ATCS/TR/6.5	Surge Protection: Built in regulated Power supply with surge suppressor & over current/ over voltage protection.	
ATCS/TR/6.6	PIV Protection: Reverse/over voltage Protection for LED Chains Operating Temperature: As per City requirement	
ATCS/TR/6.7	Operating Conditions: - Power Factor: > 0.9 - Operating Temperature: As per City requirement - Humidity: As per City requirement - Diameter: 300 mm dia – Industry Standard	
7. Solar Panels and Power Backup		
ATCS/TR/7.1	Solar Panels and power back up of 72 Hours - quantity of solar module and battery bank to be calculated keeping in view complete intersection load with Power Backup.	
8. Microprocessor Based Pedestrian Pelican Traffic Signal Controller		
ATCS/TR/8.1	Push Button control panel for pedestrian actuation traffic signal control - pole mounted type. System is also known as Call registration unit for Pelican traffic control with manual Push button switch & Indication Panel is specially designed considering safety of pedestrian traffic and works on Low voltage DC operation for safety against voltage shock.	
ATCS/TR/8.2	Visual indication: Indicator for call Register (Big push button unit having 2 Light Indicators for pedestrian signals & 1 for Call confirmation Indication (call registration /wait)	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
ATCS/TR/8.3	Audio Indication: Beep buzzer (in selective models)	
ATCS/TR/8.4	Working voltage: 12 Volts DC	
ATCS/TR/8.5	Body Material: Plastic / Metal MS Powder coated.	
ATCS/TR/8.6	Mounting: Pole mounted with help of brackets.	
ATCS/TR/8.7	Pedestrian Actuated Traffic Control Signals will be installed at places where a large number of people cross the road but on account of heavy vehicular traffic, crossing of the road is not safe for the pedestrians most of the time. Examples are near Schools, Hospitals, Shopping Centres, places of worship and similar other establishments.	
ATCS/TR/8.8	The essential equipment for the system's function will comprise of the following items: - Two sets of RED and GREEN Pedestrian Traffic Lights Signals to be installed on the two diagonally opposite corners of the Zebra Crossing. - Two sets of RED, AMBER and GREEN Vehicular Traffic Signal Lights to be installed at the Stop Lines on the Left lanes of the Road before the Zebra Crossing. - Signal posts for the Traffic signal lights - Pedestrian Actuated Stations on both ends - Pedestrian Actuated Traffic Control Unit with micro-controlled Programmer and Pedestrian Call registrations.	
ATCS/TR/8.9	When initiated, in the Actuated Mode, the system will operate as per the scheme programmed& duration of Minimum & maximum timer allotted.	
ATCS/TR/8.10	In the Actuated mode the signal sequence and timings are controlled by Pedestrian Call detectors.	
ATCS/TR/8.11	In the manual mode the signal stage is made stationery and it advances to the next stage on operation of the manual Push Button. A minimum interval of 3 seconds is fixed to avoid accidents.	
ATCS/TR/8.12	In the Automatic mode the system operates as a Fixed Time signal.	
ATCS/TR/8.13	The sequence runs at pre-set time of stages as under:	
ATCS/TR/8.14	Blink Mode – flashing of amber and Pedestrian Red.	
9. Vehicle Detection Cameras		
ATCS/TR/9.1	Camera shall provide integrated vehicle detection capability.	
ATCS/TR/9.2	The system architecture shall fully support Ethernet networking of system components through a variety of industry standard and commercially available infrastructures.	
ATCS/TR/9.3	The machine vision system hardware shall consist of three components: - Camera based vehicle detection shall be provided consisting of black & white detection camera, 640x480 resolution, 20 FPS minimum frame rate. - A modular cabinet interface unit - A communication interface panel	
ATCS/TR/9.4	The lens type shall be wide angle lens for stop line detection up to 4 lanes minimum.	
ATCS/TR/9.5	The server and client applications shall be hosted on the ATCS server that are used to program and monitor the system components.	
ATCS/TR/9.6	Both streaming video and data communications shall be available, and monitoring shall be possible from a remote workstation.	
ATCS/TR/9.7	Minimum 16 virtual loops per camera for vehicle presence detection shall be available.	
ATCS/TR/9.8	Minimum 16 detection outputs shall be available per junction.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
ATCS/TR/9.9	Filters shall be provided for tree shadow suppression.	
ATCS/TR/9.10	Facility shall be provided to assign detection output to multiple zones.	
ATCS/TR/9.11	Camera's temperature range shall be as per City requirement	
ATCS/TR/9.12	Camera's humidity range shall be up to 95% non-condensing.	
ATCS/TR/9.13	IP65 protection housing shall be provided with integrated rain/sun shield window in glass.	
ATCS/TR/9.14	High quality rust-free mounting and bolts shall be provided suitable for outdoor conditions.	
ATCS/TR/9.15	The real-time performance shall be available for observation by viewing the video output from the sensor with overlaid flashing detectors to indicate the current detection state (on/off).	
ATCS/TR/9.16	Placement of detection zones shall be by means of a laptop with the Windows 10 operating system, a wireless keyboard and a wireless mouse. The laptop's monitor shall be able to show the detection zones superimposed on images of traffic scenes.	
ATCS/TR/9.17	The detection zones shall be created by using a mouse to draw detection zones on the Laptop's monitor. Using the mouse and keyboard it shall be possible to place, size, and orient detection zones to provide optimal road coverage for vehicle detection. It shall be possible to download detector configurations from the Laptop to the field device.	
ATCS/TR/9.18	The computer's mouse and keyboard shall be capable to edit previously defined detector configurations to permit adjustment of the detection zone size and placement, to add detectors for additional traffic applications.	
10. Poles		
ATCS/TR/10.1	Standard GI Standard Signal Pole with support structure for Solar Panel	
ATCS/TR/10.2	Dimension - Length - 6000 MM - Pole diameter - 114 MM - Pipe Wall thickness - 3 MM	
ATCS/TR/10.3	Base Plate - Size 200 MM x 200 MM x 16 MM thick with foundation accessories	
ATCS/TR/10.4	Paint - Color-Galvanized Natural Finish	
ATCS/TR/10.5	Vertical GI Cantilever pole with support structure for Solar Panel	
ATCS/TR/10.6	6.50 Meters long Pole (minimum clearance from road level) having diameter 125 mm with a base plate is 300 x 300 x 20 mm. Pole sheet thickness is 4mm, with a suitable Arm length: - For 2 lane Road 3 mtrs – ARM - For 3 lane road 4.5 mtrs – ARM - For 4 Lane Road 6 mtrs – ARM	
ATCS/TR/10.7	With a thickness of 4 mm having a dia of 80mm, with suitable foundation accessories i.e. 4xM-25 x 850mm with junction box in pole. (With Steel Rope)	
ATCS/TR/10.8	More than 6500 mm above ground level including Foundation.	
ATCS/TR/10.9	All signal poles shall be placed a minimum of 0.50 meters from face of the pole to the edge of the pavement. Poles shall be as close to the intersection as practical to allow other attachments such as pedestrian equipment.	
ATCS/TR/10.10	Poles shall not be disrupting pedestrian crosswalk and/or sidewalks and shall consider any restrictions or constraints derived from utility clearances requirements.	
ATCS/TR/10.11	Traffic signal poles and their foundations shall be able to withstand a 3-second	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	gust of 145 to 240 km/h with all the equipment mounted including but not limited to traffic signal heads, pedestrian heads, solar panels, controller, battery bank, traffic signs, street name, TSP equipment, and detection equipment.	
ATCS/TR/10.12	Traffic signal poles shall be designed to endure a life cycle of 20 years.	
ATCS/TR/10.13	The hand holes shall be adequately reinforced and shall be properly covered.	
ATCS/TR/10.14	The selection of Signal pole/Cantilever/Gantry must be based on providing the signal heads in the center of the carriageway for the movement. In addition, general practices in India of using Signal Pole as primary and Cantilever as secondary must be followed; except if a signal pole satisfies the requirement better for a given location. The design must provide the details and approval needs to be obtained from the Client on these designs before proceeding to installation.	
ATCS/TR/10.15	Supply and mounting of all poles (Standard cantilever/Gantry type) and mast arms (to cover the traffic lanes as per site) needed to support traffic and pedestrian signal heads, TSP equipment and detection equipment.	
ATCS/TR/10.16	Poles shall include provision for electrical constructions in the form of holes and hand holes of adequate size positioned at least 0.3 meters above the base plate and at the mast arm mounting level.	
11. Construction and Installation Specifications		
General Construction and Installation Specifications		
ATCS/TR/11.1	The traffic signals shall be built in accordance with approved design and in compliance with specifications contained in this document.	
ATCS/TR/11.2	Existing electrical systems (traffic signal and street lighting) shall be kept in effective operation during the progress of the work, except when shutdown is authorized by the Owners Engineers.	
ATCS/TR/11.3	Owners Engineer shall be notified prior to performing any work on existing systems. Notice to the local traffic enforcement agency shall be issued and delivered prior to any operational shutdown of a traffic signal.	
ATCS/TR/11.4	All the construction materials will comply with applicable norms and regulations. The maker of cement shall be from a reputed Cement Manufacturing Company.	
ATCS/TR/11.5	The vendor shall repair any damages that are incurred during construction.	
ATCS/TR/11.6	Any permission, Right of Way (RoW) charges to be paid to the Municipal authorities shall be in the scope of work. The client shall only facilitate the necessary permissions.	
Foundations, Pull points and Manholes		
ATCS/TR/11.7	The excavations required for the installation of foundations, conduit, and pulling boxes shall be performed in such a manner as to avoid any unnecessary damage to streets, sidewalks, landscaping and other improvements. The trenches shall not be excavated wider than necessary.	
ATCS/TR/11.8	The location of existing detectors, conduits, pull boxes and other facilities shall be determined before using any tools or equipment that may damage those facilities.	
ATCS/TR/11.9	All excavations shall be filled, and sidewalks, pavement and landscaping restored.	
ATCS/TR/11.10	Concrete foundations shall rest on firm ground.	
ATCS/TR/11.11	In unpaved areas, a raised pad of portland cement concrete of the size shown on the plans shall be placed in front of each traffic controller cabinet.	
ATCS/TR/11.12	Tops of foundation for poles, and traffic signal cabinets shall be finished to curb or sidewalk grade or as directed by the owner's engineer. Conduit ends and anchor bolts shall be placed in proper position and at proper height, and anchor bolts shall be held in place by means of rigid top and bottom templates. The bottom template shall be made of steel.	
ATCS/TR/11.13	Welding shall not be performed on any portion of the body of high-strength anchor	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	bolts, anchor bars or studs.	
Conduits and Pull boxes		
ATCS/TR/11.14	Traffic signal design shall specify the location of conduits and junction boxes needed to install and operate all the traffic signal equipment including power supply, communications equipment, traffic signal heads, detectors, transit signal priority equipment, and cabinet equipment.	
ATCS/TR/11.15	Conduit design shall ensure that underground ducts and wiring are not damaged by heavy vehicles.	
ATCS/TR/11.16	Supply of all material, labour and equipment needed in the construction of conduits and junction boxes required by the traffic signals, detection system, and TSP system.	
ATCS/TR/11.17	Junction boxes shall be of non-ferrous metal and shall be of suitable sizes. Junction boxes shall have a removable cover equipped with cap screws to facilitate removal of the cover after sealing.	
ATCS/TR/11.18	Conduit shall be of the sizes shown on the design drawings approved by the client.	
ATCS/TR/11.19	The excavations required for the installation of conduit and pulling boxes shall be performed in such a manner as to avoid any unnecessary damage to streets, sidewalks, landscaping and other improvements.	
ATCS/TR/11.20	The trenches shall not be excavated wider than necessary for the proper installation of conduit and pull boxes.	
ATCS/TR/11.21	Excavation shall not be performed until immediately before installation of conduit and pulling boxes.	
ATCS/TR/11.22	The material from the excavation shall be placed in a position that will not cause damage or obstruction to vehicular and pedestrian traffic nor interfere with surface drainage.	
ATCS/TR/11.23	Unless "Trenching in Pavement Method" is specifically allowed or required in the special provisions, conduit shall be placed under existing pavement by jacking or drilling methods. Pavement shall not be disturbed without permission from the owner's engineer. In the event obstructions are encountered, upon approval of the Engineer, small holes may be cut in the pavement to locate or remove obstructions. Jacking or drilling pits shall be kept 2 feet clear of the edge of any type of pavement wherever possible. Excessive use of water, such that pavement might be undermined or sub-grade softened, will not be permitted.	
ATCS/TR/11.24	The bottoms of pull boxes installed in the ground or in sidewalk areas shall be bedded in crushed rock and shall be grouted prior to the installation of conductors.	
ATCS/TR/11.25	Trench Marker Tape shall be installed to indicate the existence of electrical wire below.	
ATCS/TR/11.26	Conductors shall be run in conduit, except overhead and temporary installations, and where conductors are run inside poles.	
ATCS/TR/11.27	All applicable environmental regulations shall be met during construction.	
Poles and Mast Arms		
ATCS/TR/11.28	Poles shall be plumbed in a way so that they are vertical when viewed from all directions. The plumb will be checked by the client's engineer and any adjustments if necessary shall be done by installing levelling shims as required around the anchor bolts.	
Switches -Field		
ATCS/TR/11.29	Each signalized intersection shall have an environmentally rugged, Layer 2, Gigabit or higher based Ethernet switch supporting full duplex communications.	
ATCS/TR/11.30	The Ethernet switches shall be compliant with IEEE 802 specification family for hardware features implemented. At a minimum, this shall include 802.3u (fast Ethernet), 802.3z (Gigabit Ethernet), 802.3x (Full Duplex with flow control), 802.3q	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	(VLAN), 802.3w (rapid spanning tree protocols), and 802.3ad (port trunking).	
ATCS/TR/11.31	The Ethernet switches shall have a minimum of 12 (ports) 10/100 Base TX or 100BaseFX ports or a combination of the two, respectively, as per the requirements.	
ATCS/TR/11.32	The Ethernet switches shall interface to the network backbone through 1000BaseFX interface.	
ATCS/TR/11.33	All field devices having distance less than 90m from the switch port shall be connected over 100BaseTX. If the distance between the device and the respective switch port is greater than 90m, either Ethernet extenders or media converters (with multi-mode fibre) for connectivity may be proposed.	
ATCS/TR/11.34	The Ethernet switches shall be interoperable with other manufactured Ethernet switches while still achieving all common Ethernet standards.	
12. Field Junction Box		
ATCS/TR/12.1	• GI with powder coated Cabinet material with min 1.2mm thickness • IP 55 to keep the temperature within suitable operating range • Mounting on Camera Pole / Ground mounted on concrete base	

Traffic Violation Detection System

Objective

In order to enhance efficiency of traffic enforcement across the city, Traffic Violation Detection System (TVDS) has been proposed across major locations in the city. TVDS detects and captures evidence of traffic violation and penalize violators remotely in order to reduce traffic accidents and enhance safety of road users. Installation of TVDS system is critical to encourage adherence towards traffic rules and regulations.

Key benefits envisaged from installation of TVDS include:

- Detects and provides evidence of traffic violation to the traffic violators enabling effective enforcement and compliance of traffic rules and regulations
- Enables city wide monitoring of traffic rules and with limited manual intervention
- Provides for penalizing the traffic violators remotely
- Reduction in violation reduces incidence of traffic accidents and enhances safety of the commuters on the road
- Bring in transparency in the system and reduces corruption
- Tamper proof system and control over redundant and duplicate work
- Enable tracking of repeated offenders

Scope of Work

The broad scope of work to be covered under this sub module shall include the following, but is not limited to:

- The MSI shall install the TVDS System at 29 traffic junctions as given in the table below across the city. This system shall capture the infractions of Red light and stop line violations, free left blocking violation at these junctions and Speed violation.
- The MSI shall design, supply, and install the TVDS system as defined in the RFPs, all wiring connections to the traffic signal controllers and to the camera platforms shall be installed by the MSI. The MSI shall supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.
- The solution proposed by the MSI shall seamlessly integrate with the E-Challan system proposed under the scope of this project. RSCL shall facilitate to get access to the Vaahan and Sarathi database. MSI shall be required to access the same through use of appropriate APIs.

- The MSI shall be responsible for providing all the necessary IT infrastructure for detection, analysis, storage & retrieval of the infraction information and number plate information at ICCC or any other location as specified in the RFP.

The proposed locations for installation of TVDS is given in the table below:

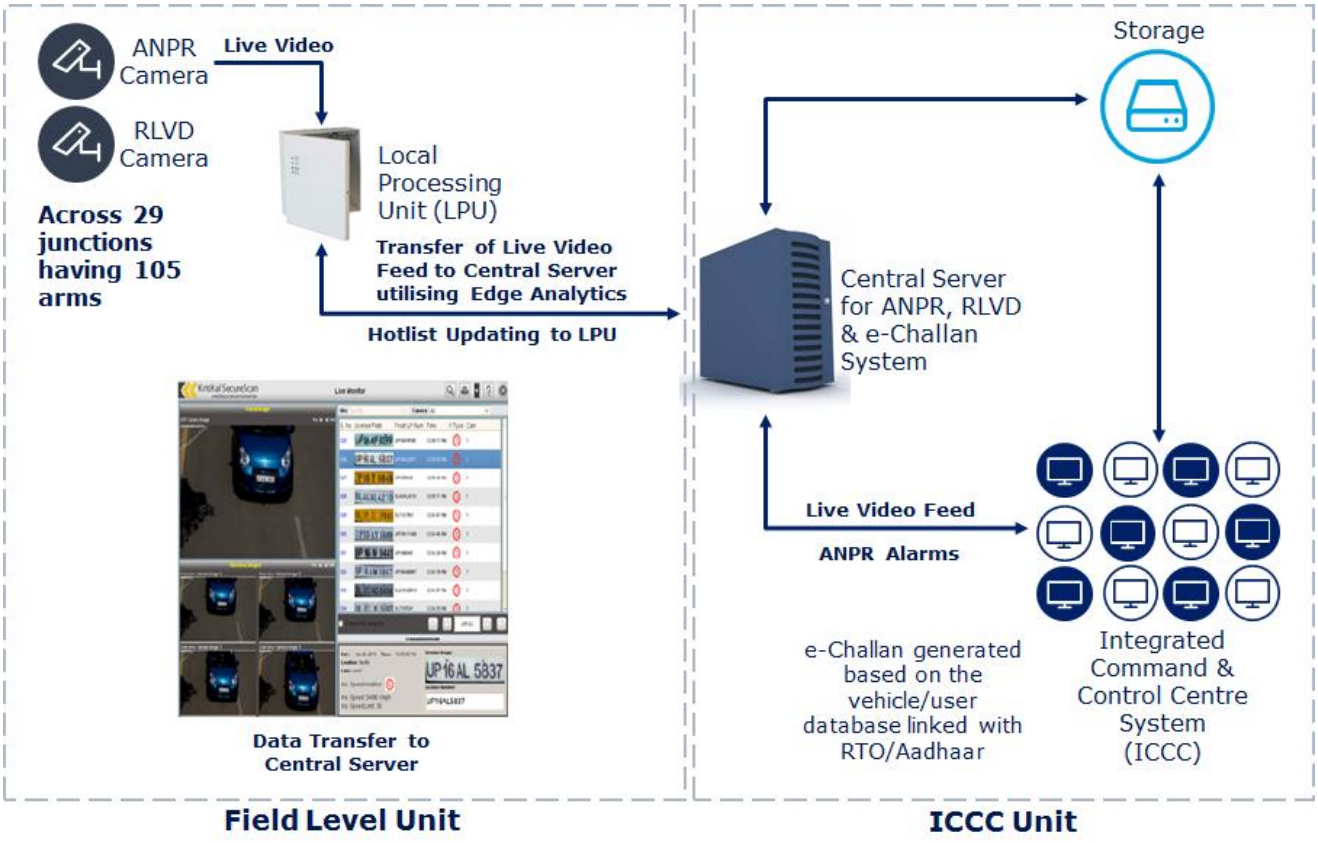
S.No.	Junction Name	Type of Junction (No. of Arms)
1	Birsa Chowk	6
2	Traffic tower	3
3	Sector-2	4
4	Ambagan Chowk	4
5	7/17 Chowk	4
6	7/15 Chowk	4
7	Sector-8	4
8	DPS Chowk	4
9	Air strip Chowk	3
10	SOS Village Chowk	3
11	Chhend Chowk	3
12	DAV Chowk	4
13	Gadiatola Chowk	4
14	Municipality Chowk	3
15	Sarna Chowk	3
16	Bania Chowk	4
17	Traffic gate	4
18	Madhusudan Chowk	4
19	Hockey Chowk	3
20	Panposh Chowk	4
21	Shani Mandir	3
22	Hi-tech Medical Chowk	3
23	Civil Township parking Chowk	3
24	Dandiapadi Chowk	3
25	Vedvyas Chowk	3
26	Rangila Chowk	4
27	Chhend BSNL Chowk	4
28	Diesel Colony Chowk	3
29	Chowdhary Petrol Pump	3

Indicative Solution Architecture

TVDS comprises detection of following types of traffic violations namely,

- Red Light Violation and Detection (RLVD): the system detects red light violation at signalized junctions and capture real time images of the vehicle and its number plate.
- Zebra Crossing Violation/ Stop Line Violation: the system detects stop line violation at zebra crossing and capture images of the vehicle and its number plate.
- Speed Violation Detection: the system detects traffic speed violators driving vehicles above the defined speed limits at road section and capture high resolution images of the vehicle and its number plate captured at high speed.
- Free Left Lane Blocking Violation: the system is capable of detecting vehicles blocking way of left moving traffic at a free left turning section of the road intersections and capture real time images of the vehicle and its licence number plate.
- Wrong Direction Vehicle Movement: capable of detecting movement of vehicles in wrong direction and capture real time images of the vehicle and its number plate.

An indicative solution architecture proposed for the installation of traffic violation detection system to enhance monitoring and ensure better enforcement of the traffic rules in the city is shown in the figure below.



The above violation detectors shall be integrated with ANPR system which processes the image or video shared by the above systems and identifies the licence number of the violator's vehicle. The system shall be linked with traffic and transport departments' database through which the system is able to identify the violator and issue e-challans against the violator using the evidence provided by the TVDS system.

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. General		
TVDS/FR/1.1	The system shall be deployed at all major signalized junction to monitor the moving traffic and enforce traffic violation.	
TVDS/FR/1.2	TVDS at a minimum shall comprise of ANPR cameras at sites/locations shortlisted, Video Image Processor with embedded software application for violation detection (like Traffic Limited Zone Infraction and Speed Limit Infraction etc.), video compression with integration to Command and Control Centre applications like violation booking and challan generation	
TVDS/FR/1.3	The system should work seamlessly with the ANPR sub-system to perform OCR (Optical Character Recognition) of the license plate characters (English alpha-numeric characters in standard fonts) and convert into machine readable format for further processing.	
TVDS/FR/1.4	The TVDS sub-system shall have an ANPR based on non-intrusive type of enforcement for detecting various traffic violations. It shall automatically detect the license plate in the captured video feed in real-time using the appropriate non-intrusive technology in each case as applicable. All the traffic violations should be seamlessly integrated with the ANPR sub-system and maintain the status of each violation till closure in the database.	
TVDS/FR/1.5	The TVDS system should instantaneously (within 4 seconds) receive the processed	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	ANPR of the violating vehicle from the ANPR sub-system.	
TVDS/FR/1.6	The system shall be operational 24x7 basis and capable of working in all-weather condition and shall work in both day and night conditions with the defined minimum accuracy levels.	
TVDS/FR/1.7	Secured connectivity for real-time data transfer between the TVDS sensors locations in the field with the central control room shall be provided along with complete hardware and networking required for the solution.	
TVDS/FR/1.8	The system shall be capable of storing JPEG image of the violating vehicle along with its license plate and enter the license plate number into the database along with date, time-stamp and site location details.	
TVDS/FR/1.9	It shall continuously store unaltered video clip of the vehicle approaching and leaving the violation location in the database.	
TVDS/FR/1.10	The system shall record all the data and should be able to play back the recorded video on real time basis.	
TVDS/FR/1.11	The system shall be able to provide search and filter option by date and type of violation.	
TVDS/FR/1.12	All the detected violation shall be captured and processed on real time basis.	
TVDS/FR/1.13	The system shall at least have 95% of violation detection accuracy as the minimum accuracy level irrespective of the type of violation, time and condition of the violation in the field.	
TVDS/FR/1.14	The system shall be able to detect any violation and create a unique case number for each violation in the field.	
TVDS/FR/1.15	TVDS shall also seamlessly integrate with e-challan sub-system which is capable of providing a legally binding court evidence following a proven and a robust procedure.	
TVDS/FR/1.16	There shall be an operator at central control room to operate the TVDS application on TVDS workstation.	
TVDS/FR/1.17	The TVDS system shall have an operations monitoring dashboard, located at the central control centre & monitored by the Control Centre operator.	
TVDS/FR/1.18	On this dashboard there shall be a schematic layout of the TVDS showing all the connected nodes on the GUI.	
TVDS/FR/1.19	The various nodes when connected & disconnected shall be represented in different colour schema on the GUI of the Control Centre operator.	
TVDS/FR/1.20	If any particular node is disconnected from the control room, the same shall raise an alarm to the Control Centre operator GUI & appropriate action shall be taken to rectify the same.	
TVDS/FR/1.21	The monitoring dashboard shall allow the Centre operator to click on any node & view the details of “operator” logged in, time duration since logged in, summary of operations performed.	
TVDS/FR/1.22	If Centre operator or any other user form control centre disable/enable/operate any active device remotely, the same shall be captured in Control Centre activity report with all details including but not limited to date , time, device, action performed etc.	
TVDS/FR/1.23	The monitoring dashboard shall show the status (connected/disconnected, faulty/working) of all logical devices (ANPR Camera, Overview camera, RLVD Sensor, other units etc.) connected to a particular node when clicking on a node from the monitoring dashboard GUI.	
TVDS/FR/1.24	The system shall be capable of detecting any fault in the installed system and notify the command center for repair and maintenance.	
TVDS/FR/1.25	In case of any fault in the devices connected to a node, or connectivity failure with a node, a pop-up message shall appear on the monitoring dashboard workstation. The operator has to acknowledge the pop-up message & report the type of fault to the maintenance team & shall record the details into the system.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
TVDS/FR/1.26	Fault assignment to the maintenance team shall be managed and controlled by the system software only. Once a fault is assigned by the control centre operator or authorized user to the maintenance team, the same shall be displayed in the maintenance module and once fault is closed/resolved by the maintenance team it shall be updated automatically (in case of active devices) or else updated manually in the software application/maintenance module.	
TVDS/FR/1.27	The access to monitoring dashboard shall be specific to the privilege of the user which can be defined in the system & shall be specific to a group/part of node locations.	
TVDS/FR/1.28	The system shall be capable of analysing the data and generating reports across traffic violation categories as desired by the client.	
TVDS/FR/1.29	The TVDS sub-system shall help in initiating public education and awareness program on automated enforcement of red light violations by media & motor driving learning schools by performing data processing on sample/ stored and simulated violations.	
2. Red Light Violation & Detection (RLVD)		
TVDS/FR/2.1	The non-intrusive RLVD sub-system should be capable of capturing multiple Infraction Vehicle Data (IVD) simultaneously on each arm of the junction at any point of time.	
TVDS/FR/2.2	The system shall be capable of identifying and capturing the vehicle traveling through the red light junction in both day and night conditions.	
TVDS/FR/2.3	The RLVD system shall be able to integrate with various transport applications in order to generate E-Challans through automated process on a real time basis after each violation.	
TVDS/FR/2.4	The system shall be capable of monitoring and detecting violation at multiple junctions at a time.	
TVDS/FR/2.5	The system shall be capable of generating reports for keeping track of violation records.	
3. Zebra Crossing Violation/Stop Line Violation		
TVDS/FR/3.1	The non-intrusive system should be capable of detecting the violations and capturing multiple IVD simultaneously on each arm of the junction at any point of time.	
TVDS/FR/3.2	The system shall be capable of identifying and capturing the vehicle violating the zebra crossing/stop line both night and day.	
TVDS/FR/3.3	The system shall be able to monitor and detect violation at multiple junctions at a time.	
TVDS/FR/3.4	The system shall be able to integrate with various transport applications in order to generate E-Challans through automated process on a real time basis after each violation.	
TVDS/FR/3.5	The system shall be capable of generating reports for keeping track of violation records.	
4. Speed Violation		
TVDS/FR/4.1	The nonintrusive system shall be capable of measuring speed of vehicles and capture over speed vehicles The Speed measurement should support multiple methods for calculation of speed – either Average or Instantaneous Speed Measurement methods.	
TVDS/FR/4.2	The system shall have the provision of setting different speed thresholds for different class of vehicles.	
TVDS/FR/4.3	The speed violations system shall be installed on mid-blocks or designated areas as	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	identified during design stage.	
TVDS/FR/4.4	The system shall be able to integrate with various transport applications in order to generate E-Challans through automated process on a real time basis after each violation.	
TVDS/FR/4.5	The system shall be capable of identifying and capturing the vehicle violating the speed limits in both night and day.	
TVDS/FR/4.6	The system shall be able to monitor and detect violation at multiple points at a time.	
TVDS/FR/4.7	The system shall be capable of generating reports for keeping track of violation records.	
5. Free Left lane blocking violation		
TVDS/FR/5.1	The non-intrusive system shall identify the violation where either the Free Left is blocked by other vehicles or violation occurred when no free left is allowed.	
TVDS/FR/5.2	The system shall be capable to mark the free left junctions (through exceptions in case fewer number exists).	
TVDS/FR/5.3	In case of blocking the “Free Left”, the system shall capture multiple IVD for the vehicles in the front area of the free left blocking the road.	
TVDS/FR/5.4	In case of “No Free Left”, the system shall be able to capture multiple IVD’s.	
TVDS/FR/5.5	The system shall be able to integrate with various transport applications in order to generate E-Challans through automated process on a real time basis after each violation.	
6. Wrong Direction Vehicle Movement		
TVDS/FR/6.1	The non-intrusive system shall be installed at critical junctions to capture the wrong direction vehicle movement. The system shall identify and capture multiple IVD.	
TVDS/FR/6.2	The system shall be able to integrate with various transport applications in order to generate E-Challans through automated process on a real time basis after each violation.	
7. Automatic Number Plate Recognition System (ANPR)		
TVDS/FR/7.1	ANPR System plays the central role in identifying the infracting vehicle from traffic violation perspective. The ANPR System identifies the number plates of these vehicles and then passed on to various other sub-systems for further processing. The system is also used for identifying the hot-listed vehicles for ensuring law & order in the city by the police department. ANPR system shall identify vehicles by their registered number plates and capture and read each vehicle number plate that passes through its field of view in multiple lanes and shall store the number in its database.	
TVDS/FR/7.2	The ANPR system shall capture the vehicle license plate from front or from rear depending on the proposed solution.	
TVDS/FR/7.3	The ANPR system should be able to detect and recognize the English alpha numeric License plates in all standard fonts and formats of all vehicle classes irrespective of the type and size of the vehicle. In addition, apart from the standard printed and High Security license plates, the system shall be able to recognize hand painted straight font alpha numeric number plates in standard formats.	
TVDS/FR/7.4	The system shall be very robust to variation in License Plates in terms of font, size, contrast and colour and work with good accuracy.	
TVDS/FR/7.5	The ANPR system shall continuously record all footage in its field of view which is to be stored at a local base station with an upload facility to the central database at command and control centre.	
TVDS/FR/7.6	The system processing shall be in real time i.e. the recognition of license plate number should happen instantaneously (within three seconds of capture).	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
TVDS/FR/7.7	The system shall be able to process and read number plates of vehicles with speeds up to 120 km/h with the minimum specified accuracy requirement.	
TVDS/FR/7.8	The ANPR shall be able to process and read the number plates at any time of the day and night, in all weather conditions with minimum specified accuracy requirement.	
TVDS/FR/7.9	ANPR system shall be integrated with the E-Challan sub-system to enable E-Challan generation and payment process.	
TVDS/FR/7.10	The ANPR sub-system shall have the following minimum accuracy levels irrespective of any other reason at the installed location for each of the vehicles in the field of view during any time of the day or night: • at a minimum of 95% vehicle detection accuracy • the system shall have a conversion accuracy of more than 85% for the detected vehicles for ANPR for standard format license plates • the system shall have a conversion accuracy of more than 70% for the detected vehicles for ANPR for non-standard format license plates.	
TVDS/FR/7.11	The following are the minimum details of the infracting vehicle to be captured: • Location Name and ID along with Latitude and Longitude. • Date & Time of the instance. • Vehicle Number plate (Captured & Processed). • Headway. • Image of the vehicle. • Direction of Travel. • Speed of the vehicle.	
TVDS/FR/7.12	ANPR system shall be integrated with the Regional Transport Authority (RTA) and other relevant database (Aadhaar etc.) to extract registered details of the vehicles based on the captured number plates. The details from the capture shall be stored & maintained in a dedicated database and at minimum, shall include the following details. • Vehicle Registration Plate Number • Date of Registration • Name of the Person of which the Vehicle is registered to • DOB of the Person of which the vehicle is registered to • Date of Renewal • Location of Issuing Registration Authority Office • Class of Vehicle • Vehicle Colour • Vehicle Insurance No. (historic and Active) • Insurance Validity Date • Vehicle Fitness No. • Fitness Validity Date • Vehicle Permit No. • Permit Validity Date • Load permit • History of Violations	
TVDS/FR/7.13	The ANPR sub-system shall be used for purpose of various add-on use-cases such as travel time estimations, estimating O-D patterns in the city, stolen vehicle identification etc.	
TVDS/FR/7.14	ANPR shall work with an analytics engine for identifying and capturing traffic violations. The system shall be able to automatically send high alert to the command and control centre for next course of action.	
TVDS/FR/7.15	ANPR system shall have the provision to detect hotlist vehicles and notify the same to the appropriate authority for requisite actions. The ANPR sub-system shall be able	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	to connect to external sources/ 3rd party databases and check each captured ANPR vehicle numbers against these sources to detect any hot-listed vehicle. Further, the ANPR system shall immediately send a configurable high-alert to the pre-designated people with details of the hot-listed vehicle and all other captured details.	
TVDS/FR/7.16	The ANPR system shall be capable of providing colour video and image evidences of infracting vehicles for purpose of supporting evidence in the court, if any. The tamper-proof video extract shall be provided as a supporting evidence (for submission in a court of law) to each infracting vehicle and the video length shall be t-5 to t+5 seconds where t being the instant at which the infraction occurred. The video output should be in colour in any industry standard format such as MJPEG, MP4, AVI etc.,) with visually readable license plate number.	
8. E-Challan System		
TVDS/FR/8.1	The e-challan System shall • Report all validated violations to a central software application deployed at the command centre leveraging the communication network • Include central reporting system at the ICCC. • Include reporting dashboards with location specific thresholds to be set for generating customized reports • Be capable of monitoring the number of vehicles based on violation type during any given time • Generate reports for any location, for each of the violations capturing challan and revenue details, and details of vehicles, repetition of violation etc. These reports should be available in all standard acceptable formats like .csv, .pdf, .txt, etc.	
TVDS/FR/8.2	The e-challan System shall facilitate real time revision of violation fees and shall enable real time communication of rules to all remote terminals from Central facility/Control Centre.	
TVDS/FR/8.3	The e-challan System shall enable client or any other appointed third party to facilitate generation of reports based on business rules to be amended from time to time.	
TVDS/FR/8.4	The e-challan System shall track each and every revenue source and shall ensure no leakages due to manual intervention.	
TVDS/FR/8.5	E-challan system shall be able to retrieve vehicle owners' details and vehicle data from RTO database to minimize data entry. Further, the E-challan system shall also retrieve data which are not available from the RTO database, by linking with the Aadhaar Database.	
TVDS/FR/8.6	E-challan system shall be able to retrieve vehicle registration details by reading Vehicle Number Plate and driving license details by reading Driving License Smart card to minimize data entry.	
TVDS/FR/8.7	While filling challans in handheld device the login authentication of the user using the handheld devices shall be done locally, so that device is usable even when there is no cellular network connectivity.	
TVDS/FR/8.8	The e-challan software shall have the provision to deny access to the Traffic police officer in the event of his suspension or for any other reason of disqualification.	
TVDS/FR/8.9	While filling challans in handheld device it shall be possible to go back to previous screen any time, edit the data and come back to present screen.	
TVDS/FR/8.10	Certain fields such as name of driver, registration number of vehicle, offence type, date, time and location should be mandatory. In case of notice files, information such as Registration number of vehicle, offence type, date, time, location, make and colour shall also be mandatory fields. No notice or challan shall be generated without filling these mandatory fields.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
TVDS/FR/8.11	Input data validation as per defined rules, must take place in the handheld device itself through client software to eliminate errors prior to transfer into the database.	
TVDS/FR/8.12	A unique challan number shall be generated through client software for each challan. The server must assign a separate primary key for each challan uploaded on the server.	
TVDS/FR/8.13	The system shall have the provision to issue challan by the Traffic officers only for the violation they are authorized to register.	
TVDS/FR/8.14	The handheld devices shall be capable of automatically checking from the server the status of the vehicle (i.e. if the vehicle is stolen, wanted in any criminal case or it is in the list of suspicious vehicles) once the vehicle registration number is entered.	
TVDS/FR/8.15	The most frequent traffic offences shall be kept at the top in the drop down menu and offence ingredients shall be available if required by officer.	
TVDS/FR/8.16	Date, time and GPS coordinates of place of challan shall be automatically populated in the relevant fields of client software.	
TVDS/FR/8.17	Compounding amount must populate in the field automatically from the master table and appropriately increase as per Motor Vehicle Act for repeat offenders. This field should not be editable by the traffic officer.	
TVDS/FR/8.18	After a challan has been printed, the officer shall not be able to change or delete any challan data even when there is no connectivity and the data has not been pushed to central server.	
TVDS/FR/8.19	Hand Held device users, other users who are connected with server and Administrator shall have full rights to change their password. Passwords must move to server in encrypted form.	
TVDS/FR/8.20	User forms and GUI of client and server software must be intuitive and easy to use and require minimal training. GUI should have menu driven combo boxes, radio buttons etc. to minimize number of key strokes.	
TVDS/FR/8.21	At any stage, context based help should be available to the user using the device. General help files should also be available in device.	
TVDS/FR/8.22	The client application shall be capable of storing data locally when off line. Data synchronization with server should take place automatically whenever network is available	
TVDS/FR/8.23	There shall be a dedicated administration module where different users or group users, having various rights and privileges as defined by administrator under IT policy, can be created.	
TVDS/FR/8.24	Only role based access to database and server shall be permitted.	
TVDS/FR/8.25	Software shall have the facility to add and manage e-challans. It should be Compatible and connected with mobile e-challan upload application installed in handheld machine.	
TVDS/FR/8.26	e-challan software shall have specific input fields like location (GPS/GPRS based) with provision of entry, Officers detail who is making challan, Vehicle number, drivers detail /License number in case of in person SPOT challan, date and time of challan, Picture upload, Violation type with dynamic challan amount and Act.	
TVDS/FR/8.27	Separate manageable/ configurable masters for Challan type (Violation type) with amount and Act shall be present.	
TVDS/FR/8.28	Provision to open transport Headquarters website for searching and entering names and address details of owner of vehicle shall be present.	
TVDS/FR/8.29	Software shall be scalable or made compatible to retrieve data from transport website NIC SARATHI /NCRB automatically using API / Web services etc. (Integration with other Headquarters needs to be facilitated).	
TVDS/FR/8.30	Software shall have facility to generate various reports related to challans within a date range, ability to filter by Offense type, map on Google for digital mapped	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	analysis, number of Challans Made for a particular person/ driving license number, number of paid / unpaid, Traffic e-challans, challans made by particular officer or all by showing Respective numbers of challans.	
TVDS/FR/8.31	With provision of vehicle type like commercial or private, either entry can be made in challan form or same can be retrieved from transport website for Reporting, verification and action about wrong permit, consecutive challans for a Particular vehicle etc.	
TVDS/FR/8.32	While making challan of any Vehicle, Software may be able to POP UP and report in detail about previous challans, if any, for the same person / vehicle.	
TVDS/FR/8.33	The data transmitted using the GSM/ GPRS or any other technology from the device to the server should be using the HTTPS (Hyper Text Transfer Protocol secure).	
TVDS/FR/8.34	Software shall be fully customizable as per user requirement as and when required.	
TVDS/FR/8.35	Software shall come with comprehensive onsite warranty for whole e-challan system including Hardware software and accessories.	
TVDS/FR/8.36	The system shall be able to monitor the functioning of all handheld machine and its critical parts. A report of faulty handheld machines or its part shall be auto generated and same may be rectified within required time.	
TVDS/FR/8.37	The e challan system shall be able to integrate with TVDS (Traffic violation detection) system. All challan generated through TVDS shall be recorded in to the e challan system.	
TVDS/FR/8.38	The "e-challan system" shall generate the hash value of the each e-challan (files including image, video, transection detail, data entry) generated by the system, Print on the slip and store in the system also.	
TVDS/FR/8.39	The e-challan system shall be able to generate e-challan signed digitally by Digital signature of the responsible authority.	
TVDS/FR/8.40	The e-challan system shall be available online for the officer sitting at the control room. It shall be possible to generate e-challan for the violations observed through the Camera footage being streamed from City surveillance system or TVD system. The e-challan system shall be able to record the selected evidence for the e-challan.	
TVDS/FR/8.41	Daily backup facility the e-challans shall be present. Facility to export and store the same to external device shall be present.	
TVDS/FR/8.42	The e-challan system software shall at a minimum comprise the following - Photo Collection - Violation booking - e-challan Generation - Postal dispatches - Postal Statement - Postal returns and return info feeding - Data entry in vehicle Registration remarks database - Provision to enter comment Sold out vehicles/Fake vehicles /Fake addressed - Vehicles/Theft Vehicles/Authorized complaints/Multiple owners) - Identification of Police Stations, Junctions, Courts, Police Staff for the Traffic dept. - MV Act cases - ID, Address & contact details fields addition. - Action dropouts as per Court decisions - Report Generation - Online Pending Challan Verification - Online Violation photo view facilities - Upgrading the E-challan Software	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Online Uploading photos by the Police in Control room - Online handheld machine tracking System - Server database and crash recovery of data. - Regular Backup System - Performance tuning of the Application, Database tuning, Network tuning, Web Service tuning. - Traffic violators History (for suspension of driving license) - APIs for sharing e-Challan information for online payment and updation of payment status in e-Challan application server. - Generating hash value for each challan - Digital signing of challan	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
1. Automatic Number Plate Recognition			
TVDS/TR/1.1	Image Sensor	1/3” or better Progressive Scan CMOS	
TVDS/TR/1.2	Min. Illumination	0.01 lux color, 0.001 lux b/w, 0 lux with IR	
TVDS/TR/1.3	Shutter Speed	1s-1/30,000s	
TVDS/TR/1.4	Lens	5-50mm	
TVDS/TR/1.5	Day & Night	IR Cut Filter	
TVDS/TR/1.6	Auto-iris	DC drive	
TVDS/TR/1.7	WDR	120db	
TVDS/TR/1.8	SNR	≥ 50dB	
TVDS/TR/1.9	Video Compression	H.264, H.265 and H.265/MJPEG/ MPEG-4 or better	
TVDS/TR/1.10	Video Bit Rate	32 Kbps – 8 Mbps	
TVDS/TR/1.11	Audio Bit Rate	G7.11 or better	
TVDS/TR/1.12	Max. Resolution	1920 x 1080 @ 25-60fps (2 Megapixel)	
TVDS/TR/1.13	Video Streams	Triple	
TVDS/TR/1.14	Image Enhancement	BLC, 3D DNR, ROI	
TVDS/TR/1.15	Image Setting	Rotate Mode, Saturation, Brightness, Contrast, Sharpness adjustable by client software or web browser	
TVDS/TR/1.16	Day/Night Switch	Auto	
TVDS/TR/1.17	Alarm Trigger	Motion detection, Tampering alarm, Network disconnect, IP address conflict,	
TVDS/TR/1.18	Protocols	TCP/IP, UDP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, , RTP, RTSP, RTCP, , NTP, UPnP, SMTP, SNMP, 802.1X, QoS, IPV4/Ipv6	
TVDS/TR/1.19	Security	User Authentication, Watermark, IP address filtering	
TVDS/TR/1.20	Audio (-S)	1-ch 3.5 mm audio in (Mic in/Line in) /out interface	
TVDS/TR/1.21	Communication Interface	1 RJ45 10M/100M Ethernet port	
TVDS/TR/1.22	Alarm (-S)	1 input, 1 output	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
TVDS/TR/1.23	ONVIF Compliant	Profile S & G	
TVDS/TR/1.24	On-board Storage	Built-in Micro SD/SDHC/SDXC slot, up to 128 GB. The vendor should provide 128GB SD Card for the same.	
TVDS/TR/1.25	Protection Level	IP66 and IK10	
TVDS/TR/1.26	Operating Conditions	As per City requirement	
TVDS/TR/1.27	Power Supply	12 V DC ± 10% / 24VAC, PoE (802.3at).	
TVDS/TR/1.28	IR Distance	50m or more (External only)	
TVDS/TR/1.29	Regulatory	CE/FCC/EN/BIS/IS and UL certified	
2. Red Light Violation Detection			
TVDS/TR/2.1	General	The system should be capable of generating a video & minimum 3 snapshot in any of the standard industry formats (MJPEG, JPG, avi, mp4, mov, etc) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (being the instant at which the infraction occurred).	
TVDS/TR/2.2	Video Compression	H.264, H.265 /MJPEG/ MPEG-4 or better	
TVDS/TR/2.3	Video Resolution	3 Megapixel	
TVDS/TR/2.4	Frame rate	Min. 45 fps or better	
TVDS/TR/2.5	Image Sensor	1/3” or better Progressive Scan CCD / CMOS	
TVDS/TR/2.6	Lens Type	Varifocal, C/CS Mount, IR Correction full HD lens Auto IRIS	
TVDS/TR/2.7	Lens#	5~50mm /8 – 40 mm, F1.4	
TVDS/TR/2.8	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)	
TVDS/TR/2.9	IR Cut Filter	Automatically Removable IR-cut filter	
TVDS/TR/2.10	Day/Night Mode	Colour, Mono, Auto	
TVDS/TR/2.11	S/N Ratio	≥ 50 Db	
TVDS/TR/2.12	Auto adjustment	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Ture Wide Dynamic Range	
TVDS/TR/2.13	Audio	Audio Capture Capability, G.711, G.726	
TVDS/TR/2.14	Local storage	Micro SDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.	
TVDS/TR/2.15	Protocol	IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF Profile	
TVDS/TR/2.16	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption	
TVDS/TR/2.17	Operating conditions	As per City requirement	
TVDS/TR/2.18	Casing	NEMA 4X / IP-66, IK10 rated	
TVDS/TR/2.19	Intelligent Video	Motion Detection & Tampering alert	
TVDS/TR/2.20	Alarm I/O	Minimum 2 Input & 1 Output contact for 3rd part interface	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
TVDS/TR/2.21	Certification	UL/EN, CE,FCC	
On site-out station processing unit communication & Electrical Interface (Junction Box)			
TVDS/TR/2.22	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days 24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.	
TVDS/TR/2.23	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.	
TVDS/TR/2.24	Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.		
TVDS/TR/2.25	The system should be capable of working in ambient temperature range as per City requirement		
TVDS/TR/2.26	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).		
TVDS/TR/2.27	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).		
Violation Transmission and Security			
TVDS/TR/2.28	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the TCC electronically through GPRS based wireless technology with 3G upgradable to 4G, or wired connectivity if available in Jpeg format		
TVDS/TR/2.29	Advanced Encryption Standard (AES) shall be followed for data encryption on site and TCC, and its access will protected by a password.		
TVDS/TR/2.30	The vendor shall ensure that the data from the onsite processing unit shall be transferred to TCC within one day.		
Video Recording			
TVDS/TR/2.31	The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should point of time the local storage at the base station should have the data of previous 7 days.be noted that at any		
TVDS/TR/2.32	Direct extraction through any physical device like USB flash drive , Portable Hard disk etc. shall be possible		
3. IR Illuminators			
TVDS/TR/3.1	Range	Min. 100 meters, with adjustable angle to cover the complete field of view at specified locations	
TVDS/TR/3.2	Minimum Illumination	High sensitivity at Zero Lux	
TVDS/TR/3.3	Power	Automatic on/off operation	
TVDS/TR/3.4	Casing	NEMA 4X / IP-66 rated	
TVDS/TR/3.5	Operating conditions	As per City requirement	
TVDS/TR/3.6	Certificate	CE, FCC, UL/EN	
4. e-challan Devices			
TVDS/TR/4.1	The e-challan handheld shall have latest mobile operating system (Android, Windows and iOS)		
TVDS/TR/4.2	The hand held shall have latest and high speed processor with minimum frequency of 800 MHz that suits the operating system		
TVDS/TR/4.3	The device should have a minimum of 512MB RAM for smoother functioning		

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
TVDS/TR/4.4	The handheld should have 1 GB Flash or higher, with an expandable micro SD card which supports capacity of at least 32 GB		
TVDS/TR/4.5	The device shall have colour display of minimum 4 inch, with minimum resolution of 640 x 480 (with Trans reflective screen VGA/QVGA)		
TVDS/TR/4.6	The handheld device shall have capacitive Touch Screen feature for easy navigation and usage		
TVDS/TR/4.7	The device should have a sim card slot to support 4G networks		
TVDS/TR/4.8	The handheld shall support communications through all of the following • USB 2.0 or higher • RS232 Port • Bluetooth 2.0 or higher • WLAN (IEEE 802.11 b/g/n) • GSM/GPRS/EDGE/CDMA/3G/4G		
TVDS/TR/4.9	The handheld should last for minimum 8 hours of use in the field and be capable to hold 168 hours of transaction data. The device shall have suitable mechanism for charging from 220V standard AC power supply through standard power jack. The device standby time shall be for 5 days without intermittent charging. Suitable Vehicle charger shall also to be provided		
TVDS/TR/4.10	The handheld shall have in-built thermal printer and should be able to print on a paper with minimum width of 3 inch. It shall support print speeds of at least 200 dpi, 60 mm per second or better with easy paper loading mechanism. The media type shall be Thermal Paper.		
TVDS/TR/4.11	The handheld shall be able to scan 1D and 2D barcodes (QR Codes)		
TVDS/TR/4.12	The device shall have a minimum of 5 MP camera with flash that can support still images and videos in all lighting conditions		
TVDS/TR/4.13	The device shall have QWERTY keypad as mode of input		
TVDS/TR/4.14	The handheld should be equipped with a speaker emitting output of at least 10 watt and a 3.5mm audio jack		
TVDS/TR/4.15	The handheld device shall have indicators on device for power, charging, low battery, connectivity, Read/write status, etc.		
TVDS/TR/4.16	The device shall have a rechargeable type Li-ion battery with minimum capacity of 3000 mAh		
TVDS/TR/4.17	The handheld shall pass Ingress protection class/rating IP54		
TVDS/TR/4.18	The handheld device shall meet the following Operating Conditions • Temperature: As per City requirement • Operating Humidity: As per City requirement		
TVDS/TR/4.19	The device shall have all the following features • Login through unique ID • Password or biometric authentication		
TVDS/TR/4.20	E-challan software shall be installed on the handheld machines to process challans in online and offline modes per user requirement		
TVDS/TR/4.21	The device should have PCI , EMV certified as per RBI guidelines for accepting payment through Credit/Debit card and smart card		
TVDS/TR/4.22	Each of the handheld device shall come with the following Accessories • User manual • Additional battery • Disc for device driver software • Charging Adapter • Car Charger		

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
	• Device cover casing		
TVDS/TR/4.23	The handheld shall have a minimum life of 3 years under normal operational conditions.		
5. Field Junction Box			
TVDS/TR/5.1	Size	Suitable size as per site requirements to house the field equipment	
TVDS/TR/5.2	Cabinet Material	GI with powder coated	
TVDS/TR/5.3	Material Thickness	Min 1.2mm	
TVDS/TR/5.4	Number of Locks	Two	
TVDS/TR/5.5	Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake	
TVDS/TR/5.6	Mounting	On Camera Pole / Ground mounted on concrete base	
TVDS/TR/5.7	Form Factor	Rack Mount/DIN Rail	
TVDS/TR/5.8	Other Features	Rain Canopy, Cable entry with glands, proper earthing and Fans/any other accessories as required for operation of equipment's within junction box.	
6. Cables for Traffic Cameras			
TVDS/TR/6.1	No's of core	7 and 14 core 1.5 sq. mm.	
TVDS/TR/6.2		3 Core 2.5 sq. mm.	
TVDS/TR/6.3	Materials	PVC insulated and PVC sheathed armored cable with copper conductor of suitable size as specified in BOQ.	
TVDS/TR/6.4	Certification	ISI Marked	
TVDS/TR/6.5	Standards	Indian Electricity Act and Rules	
TVDS/TR/6.6	IS:1554	PVC insulated electric cables (heavy duty)	
7. Poles for Traffic Cameras			
TVDS/TR/7.1	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)	
TVDS/TR/7.2	Height	5-10 Meters (or higher), as-per-requirements for different types of cameras & site conditions	
TVDS/TR/7.3	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)	
TVDS/TR/7.4	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole	
TVDS/TR/7.5	Bottom base plate	Minimum base plate of size 30x30x1.5 cm	
TVDS/TR/7.6	Mounting	To mount RLVD Cameras	
TVDS/TR/7.7	Paint	Pole painted with two coats of zinc chromate primer and two coats of golden yellow Asian apostolate paint or otherwise as required by architect and in addition bituminous painting for the bottom 1.5 m portion of pole.	
TVDS/TR/7.8	facilities	ANPR, Speed detection sensors, CCTV cameras, Traffic Signals, Pedestrian Signals, Switch, etc.	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
TVDS/TR/7.9	Pipes, Tubes	All wiring should be hidden, through tubes/pipes. No wires shall be visible from outside.	
TVDS/TR/7.10	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds (at least 150kmph withstanding) in different climatic conditions). Expected foundation depth of min. 100cms.	
TVDS/TR/7.11		Please refer to earthing standards mentioned elsewhere in the document.	
TVDS/TR/7.12	Protection	Lightning arrester shall be provided, to protect all field equipment mounted on pole.	
8. Online UPS for field location			
TVDS/TR/8.1	Capacity	Adequate capacity to cover all above IT Components at respective field locations	
TVDS/TR/8.2	Technology	IGBT based PWM	
TVDS/TR/8.3		Technology, True Online UPS	
TVDS/TR/8.4	Input Frequency Range	45 to 55 Hz	
TVDS/TR/8.5	Output Frequency Range	45 to 55 Hz	
TVDS/TR/8.6	Output Voltage	220VAC -	
TVDS/TR/8.7		230VAC	
TVDS/TR/8.8	Voltage Regulation	+/-2% (or better) and with built- in Over Voltage Cut off facility in the Device	
TVDS/TR/8.9	Frequency	50 Hz +/- 0.1%	
TVDS/TR/8.10		(free Run Mode)	
TVDS/TR/8.11	Harmonic Distortion (THD)	< 3% (linear load)	
TVDS/TR/8.12	Output Waveform	Pure Sine wave	
TVDS/TR/8.13	Output Power Factor	0.8 or more	
TVDS/TR/8.14	Battery Backup	Adequate and required battery backup to achieve required uptime of field device as well as SLA of the overall solution.	
TVDS/TR/8.15	Battery Type	Lead acid, Sealed Maintenance	
TVDS/TR/8.16	General Operating Temperature	As per City requirement	
TVDS/TR/8.17	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection	
TVDS/TR/8.18	Bypass	Automatic, Manual Bypass Switch	
TVDS/TR/8.19	Certifications	For Safety	
		& EMC as per international standard	
TVDS/TR/8.20	Overall Protection	IP 55,	
TVDS/TR/8.21		Junction Box design should ensure to keep the temperate re within suitable operating range for equipment 's and should also avoid intentional water splash and dust intake	

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
	Parameter	Minimum Requirement	
9. Structured Cabling Component			
TVDS/TR/9.1	Standards	ANSI TIA 568 C for all structured cabling components	
TVDS/TR/9.2	OEM	OEM Certification and Warranty of 15-20 years as per OEM standards	
TVDS/TR/9.3	Warranty		
TVDS/TR/9.4	Certification	UL Listed and Verified	
TVDS/TR/9.5	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's	
10. System Administration			
TVDS/TR/10.1	The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.		
TVDS/TR/10.2	The System Administration Server shall support different logs related to the Management Server. • The System Log • The Audit Log • The Alert Log • The Event Log		
TVDS/TR/10.3	Rules: The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as: • Start and stop recording • Set non-default live frame rate • Send notifications via email Pop-up video on designated Client Monitor recipients		

City Governance

Context

Presently, the use of online system for delivery of citizen services are limited to the modules of e-Municipality and e-Abhijoga (Grievance Redressal Portal). The Odisha e-Municipality services is a centralized integrated application which provides “Single Window” services to citizens on anytime, anywhere basis. There are several stand-alone IT systems created over time under the different programs. Indicative list of such systems along with the associated vendors is provided in the table below:

Module	TCS	CSM	BSNL	NIC	CMGI/GA Dept
Solid waste management (with GPS)			Y		
Grievance redressal	Y	Y		Y	
Property tax	Y				
Trade license	Y				
Marriage Registration	Y				
HR & Payroll System					Y
Birth & death	Y				
Accounts	Y				
Audit	Y				
Right to Information (RTI)				Y	
Portal	Y				
MIS	Y				
Integration of Odisha online with e- municipality	Y				
Implementation of UC Management module	Y				
Integration of e-Taal with e-Municipality	Y				
Digitally signed and bar coded certificates	Y				
Integration of e-Mail and SMS	Y				

However, it is observed that only the online modules of Birth/Death, Trade License and Marriage Registration are presently operational in Rourkela Municipal Corporation (RMC). Further, in the e-Abhijoga grievance platform, back-end processing of grievances related to municipal services are done manually since the back-end of the grievance platform is not functional.

Objective

The overall objective of this module is to improve interaction between the city administration and residents and other city dwellers, with an overarching objective of making urban services more accessible for all providing access through multiple channels e.g., web platform, citizen facilitation centers, e-Kiosks, Mobile Application, etc. Key objectives of this module include:

- Establishing a digital platform for government and citizen interaction.
- Improving the quality of services offered to local citizens and bring up the service levels.
- Improving the internal management of the agencies providing citizen services.
- Promoting administrative functions to be carried over online.
- Engage citizens in the process of Governance through interaction.
- Empower citizens through access to knowledge and information and make the working of the government more efficient and effective.
- Enhanced transparency, convenience and empowerment; less corruption; revenue growth; and cost reduction.

The key benefits envisaged as part of the project, include:

- Rourkela shall have a comprehensive suite of e-Governance applications which shall provide convenient, anytime, anywhere citizen and employee services.

- Along with e-Governance system, Enterprise Content Management System, citizen engagement systems (including redressal, collaboration, contact centre), ICCC, KPI and dashboard system and integration of all existing systems and ready framework for integration of any future system shall be implemented. All these systems shall have a tightly integrated application architecture which shall play a vital role in not only just enhancing efficiencies for city operations but also when integrated with the citizen facing e-governance applications, shall provide the benefits of a holistic solution.
- e-Governance system shall provide significant improvement in Government to Customer (G2C), Government to Employee (G2E), Government to Business (G2B) & Government to Government (G2G) interfaces and shall streamline, standardize electronic information gathering & access, and shall increase transparency, accessibility and efficiency of the stakeholder agencies.
- e-Governance system shall facilitate information reuse, across and within various departments of the stakeholder agencies and shall reduce system maintenance and training requirements by adopting standard systems and processes for the stakeholder agencies.

Scope of Work

There are several stand-alone IT systems created over time under the JNNURM & NMMP programs. The MSI may examine these initiatives and where possible integrate them seamlessly with the proposed solution. The specifications given in this RFP are the functional requirements of RMC/RDA and the MSI should study the same, see the efficacy of current systems and then utilize, modify or replace existing systems. The MSI has to study the working of RMC/RDA, suggest and discuss BPR and then come to the to-be processes.

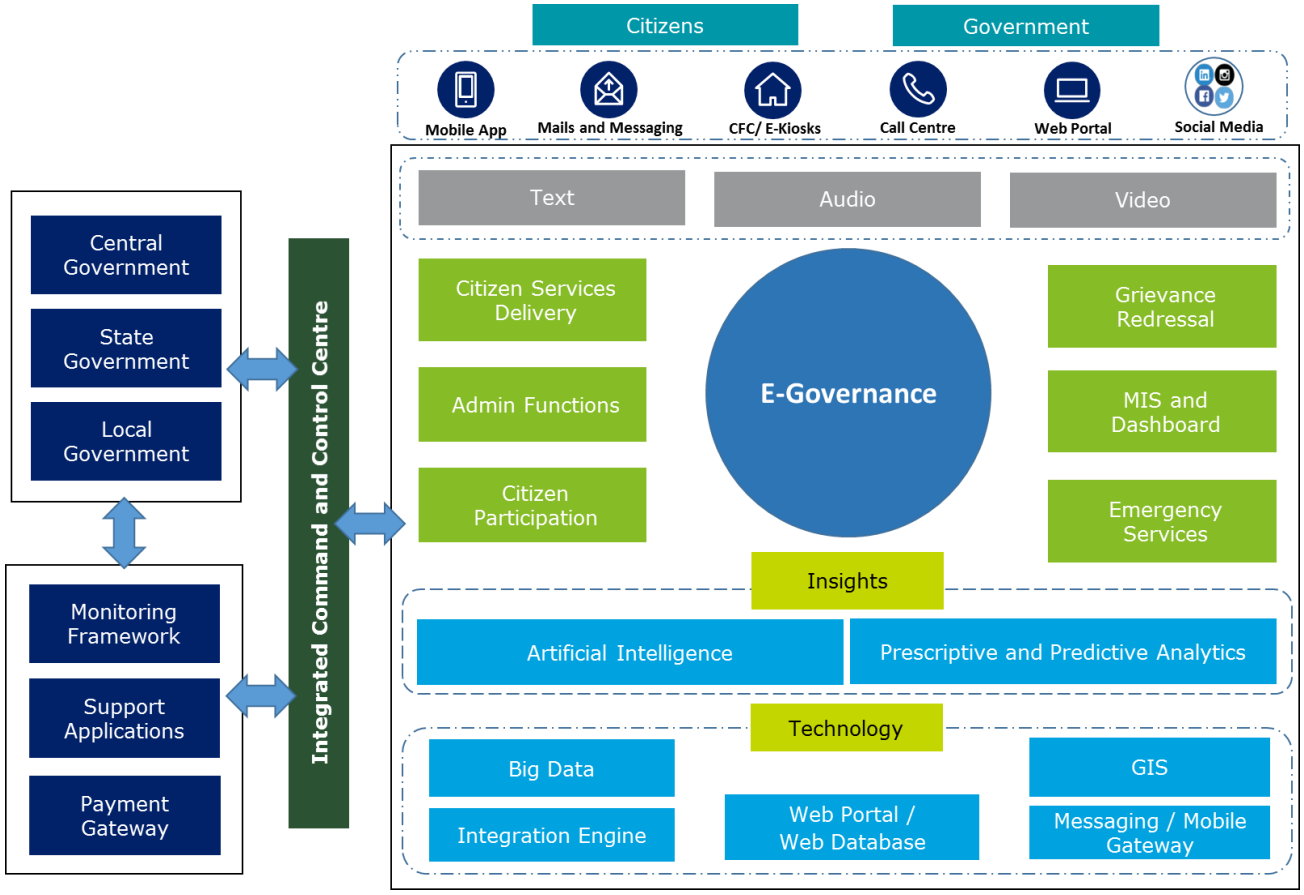
To this end, the MSI shall be responsible for complete ‘As-Is’ analysis of the existing systems with the Client. The MSI shall review the business operations of these existing systems and recommend the ‘To-Be’ scenario to the Client. The Client at its discretion may decide to continue using the existing systems or procure a new system from the MSI as part of this contract. All ‘change management’ from the as-is to the to-be scenario shall be a part of this project. The key requirement from the MSI as part of the City Governance module shall entail the following:

- All the services provided by Rourkela Municipal Corporation (RMC) / Rourkela Development Authority (RDA) shall be available online to the citizens
- One Stop Web Portal for all citizen services with links to other Govt. Department websites like WESCO, PHEO, Housing & Urban Development Department, etc.
- Online payment for citizen services and utility services using Net Banking, Credit Cards, Debit Cards, e-Wallets, etc.
- Multiple channels for delivery of these services through online web portal, Integrated Citizen Facilitation Centers, e-Kiosks, Mobile Applications, etc.
- E-Governance system shall be scalable to accommodate future growth and support hardware and software additions and upgrades.

The MSI needs to examine the existing e-Governance initiatives undertaken by Housing & Urban Development Department of Government of Odisha and integrate them seamlessly with the proposed solution. Support as and when required from the developers, will be facilitated by the State/City Government. For the purpose of integration with existing services, estimates of data migration and transactions in the existing system is given in Annexure C

Indicative Solution Architecture

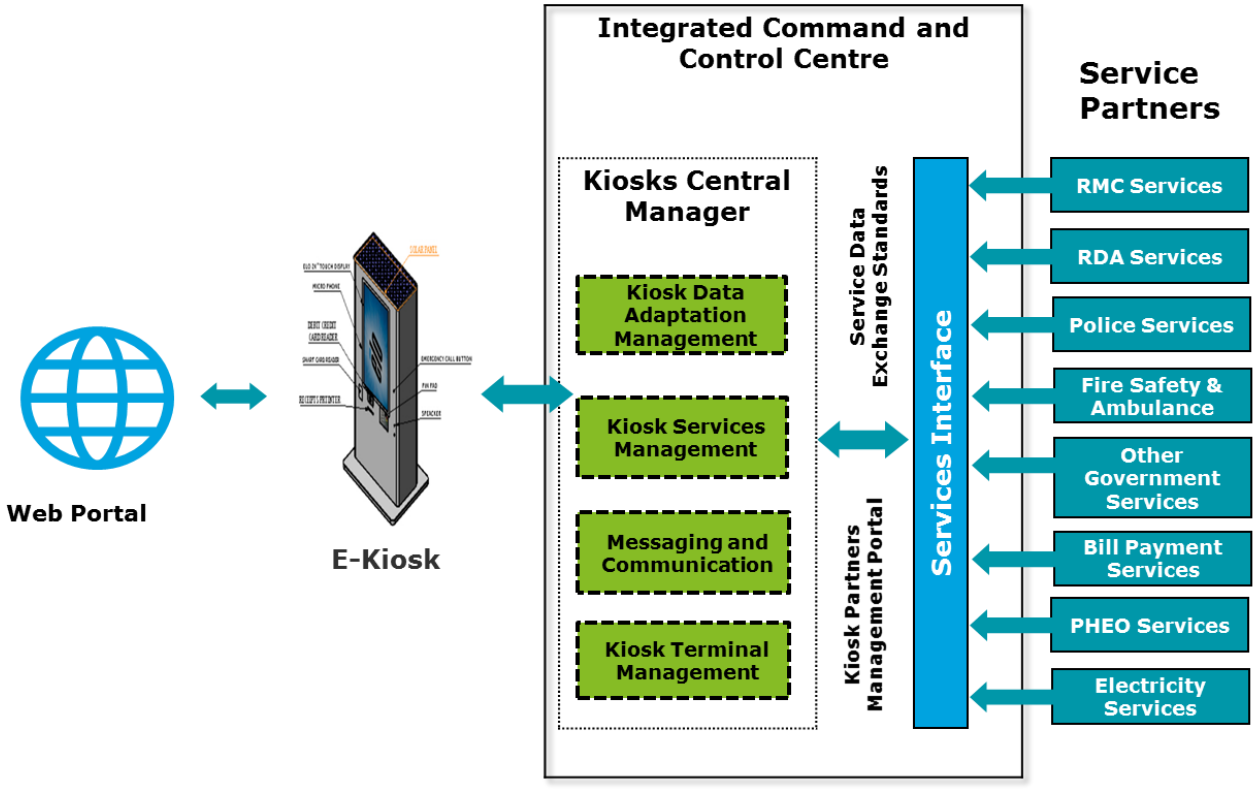
A high level schematic architecture proposed for the e-Governance project to streamline and enhance urban service delivery to the citizens in the city is presented in the figure below:



All the RMC and RDA citizen services shall be provided online to the citizens through different modes like Mobile Application, e-Kiosks, CFCs, etc.

Integrated Citizen Facilitation Centers and e-Kiosks

Multi-Services Digital Kiosk shall be connected with the ICCC using the fibre optic infrastructure. A switch shall be housed inside each multi-services digital kiosk from where the data will be backhauled to the nearest POP over the fibre optic infrastructure. An indicative schematicl architecture for the integrated multi-services digital kiosks has been presented below:



Kiosk Terminal Management

This module shall facilitate controlling of end terminals deployed across various locations. Functionalities which are expected to be part of this module include:

- Kiosk deployment details such as unique id, IP address, form factor, components included, and others
- Kiosk terminal health monitoring – health of kiosk components, whether equipment is functional or requires replacement
- Maintenance & support module – controlling maintenance of various components within kiosk, ensuring periodic maintenance as per schedules defined at the time of planning
- Upgrade of firmware, OS and other related platforms
- Management, upgradation, deployment and maintenance of various applications /API's through central location which shall then be populated across all the field located kiosks.
- Replenishment of consumables including receipt printers, open city cards
- Maintaining details of money collected by kiosk, items put in drop box and others
- Data encryption and data security within kiosk terminal

Kiosk Services Management

This module shall facilitate management of services provided through City Kiosk. It is envisaged that based on the location of the City Kiosk, services shall be configured on the end terminal. Functionalities which are expected to be part of this module include:

- Service portfolio management across all City Kiosks, services which are operational, being tested (in pilot) or in pipeline
- Enabling and disabling of services based on information received from partner management portal
- Monitoring finances, accounts, billing and payments related to services to partners

- Managing of advertisements and other promotional messages being displayed through City Kiosk
- Managing survey and feedback on various City Kiosk services
- Ensuring delivery of services detailed in subsequent sections
- Any other functions related to services delivery through City Kiosk

Kiosk Partner Management Portal

This shall be the interface for all partners (read: entities using kiosk for service delivery).

- This includes government agencies such as RMC, police, etc. Each partner shall be registered on the portal and shall have an account through which various services can be enabled / disabled / configured on basis of portal. The portal shall be single window interface for all interaction for partners with City Kiosk. Payments, bills, refunds, account statements, grievances for partners shall be managed through this portal.

Services Interface

This module shall enable interfacing with partners for providing of services. Functionalities which are expected to be part of this module include:

- Information exchange from City Kiosk terminal with partner system
- Payment gateway system with banks and intermediaries

Service Data Exchange Standards

This shall be metadata repository of various standards which may be established with multiple partners. Interface with various service providers, develop standards for information exchange as required for delivery of services through City Kiosk machines. Open standards for data exchange shall be preferred.

City Kiosk Data Adaptation Management

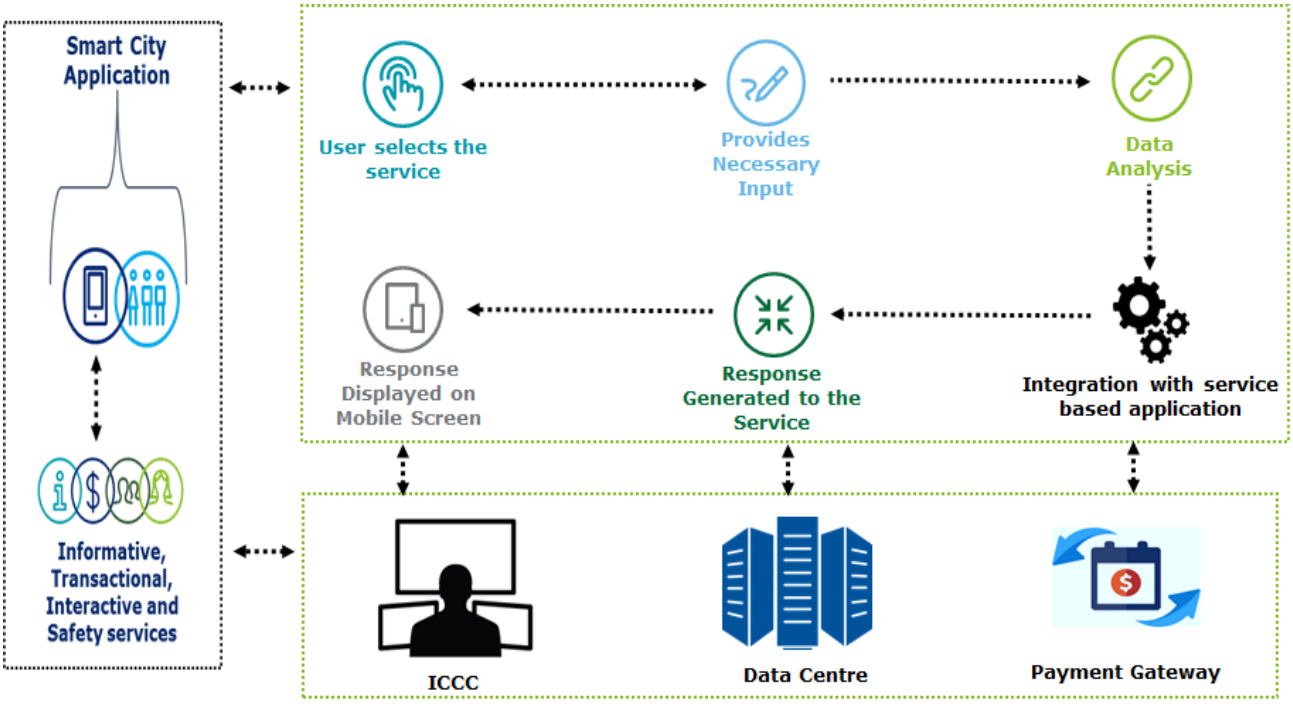
Considering the series of different inputs and related information being exchanged through City Kiosk, this component is expected to manage conversion of data as per exchange standards required. This component shall closely work with service interface and message and communication modules.

Message and Communication

This module is expected to manage message and communication between various modules within the overall system.

Mobile Application

An indicative solution architecture proposed for the Mobile application for enabling access to various services to the citizens in the city is presented in the figure below:



The typical process flow for usage of application by the users will be as follows:

- User registers and logins to the application to request for informative/transactional/interactive/safety services
- Depending upon the request the backend infrastructure interacts with necessary application to provide the desired output to the user
- The user will be able to see the necessary output as per the request on the mobile screen.

Minimum Functional Requirements

Integrated Business Process Management Services

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. Website		
EGOV/FR/1.1	The existing web sites of RMC and RDA shall be revamped and new website to be developed for RSCL. The following details are given for RMC. The same can be extrapolated for all three.	
EGOV/FR/1.2	Home Page: A clean, visually compelling home page that quickly conveys to the visitor Rourkela and what the RMC does.	
EGOV/FR/1.3	It would include (not limited to): - Home page includes About Rourkela, Message from the CEO - Link to the portal, Online Services information - Investment opportunities - Information for tourists - GIS map, Holiday List - Photo Gallery, Acts, Rules, etc. - Budget Documents, FAQs - Emergency Services and Weather information - Tenders - Key statistics - Citizen Charters - GIS map - Links to Facebook, twitter etc. with integration of social governance. - Feedback - Contact Details with Organisation Structure - Log in - Search - News & Updates, ULB Resolutions, Careers - Project Details – Status of all Projects being executed - Track count of visitors in the website	
EGOV/FR/1.4	Corporate Branding: Clearly communicates a sense of ‘identity’ at first glance.	
EGOV/FR/1.5	Visual appeal: The site must have an attractive mix of text, images, audio and video.	
EGOV/FR/1.6	Fast Loading Pages: Optimization of web pages for a faster browsing experience with compatibility with key industry browsers and platforms.	
EGOV/FR/1.7	Responsive Design: The site must be mobile-optimized through responsive design methods. Therefore, it should detect that a mobile device is being used and present the user with the mobile version first. The user should be able to switch to the desktop version.	
EGOV/FR/1.8	Simple and clear navigation: The site should be easy to navigate. Information should be grouped and presented in a logical manner and require no more than three levels of “drill down” for the user to find the desired information thus creating a clean, clear, easy and satisfying user experience. This should include drop down menus, so that the visitor can easily find what they are looking for with a few clicks of the mouse.	
EGOV/FR/1.9	Search Tools: Provide search capabilities using key words or phrasing that will	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	provide access to content from throughout the site. Additionally, make it possible to download historical and recent data whereby the user can define his/her preference.	
EGOV/FR/1.10	Select a platform that allows users to search content of the website easily and quickly without the need for extremely high speed devices (desktop, laptop and mobile) and high speed internet access.	
EGOV/FR/1.11	Links: Links should be placed within the website to allow individuals to contact institutions affiliated with the RMC and access to the portal as well the respective Ministries (can be called Useful Links).	
EGOV/FR/1.12	Easy access to Key performance indicators: Seamless integration with RMC's dashboard data to provide continuously updated graphs and charts. This will be decided with RMC input & consent.	
EGOV/FR/1.13	News/Update feed: Constant and dynamic update feed on site home page. Displays announcements and notifications for new content additions on front page of site.	
EGOV/FR/1.14	Calendar: A dynamic calendar that displays events as well as filters for searching/sorting events.	
EGOV/FR/1.15	Contact Form: Provides a web-based contact form with anti-spam controls.	
EGOV/FR/1.16	Automated e-mails: automatically send follow-up emails to our stakeholders (subscribers) if they visited a specific web page, or completed some specific task (e.g. survey) on the website.	
EGOV/FR/1.17	Social Media Engagement Tools: New tools to improve interaction with social media	
EGOV/FR/1.18	Blog: The site should have a Blog section to facilitate discussions on various topics.	
EGOV/FR/1.19	Career: The site should have a career section which should accept online job application that would be fed directly into the HRM system.	
EGOV/FR/1.20	Language Options: The website ought to be easily translated into other languages – English, Hindi & Oriya	
EGOV/FR/1.21	Citizen Mobile app: The site should allow for the download of a Citizen Mobile app. The app should be compatible with Android and iOS.	
EGOV/FR/1.22	Compatibility: Site must be compatible with Google Chrome, Microsoft® Internet Explorer 8.0 or higher, Microsoft Edge, Mozilla Firefox, and Safari 5.0 or higher.	
EGOV/FR/1.23	Mobile Access: Site must be "responsively designed" to accommodate mobile users. This must include accommodations for slower, cellular internet connections. This includes compatibility with iOS, Android and other industry standard platforms.	
EGOV/FR/1.24	Settings: Website must not require plug-ins as a default.	
EGOV/FR/1.25	Performance: Site must be able to handle multimedia (video) with high performance.	
EGOV/FR/1.26	HTML Compliance: Full compliance with HTML 5.0 or higher.	
EGOV/FR/1.27	Parallel sites: After 'Go Live' there should be two (2) sites running parallel, one for testing purposes and the other for production. All maintenance should be carried out in the test environment and be approved before migrating to the live environment.	
EGOV/FR/1.28	Easy Maintenance: Site should be easy to maintain, site should not require significant investment of time to keep site up and working with quick and easy fixes site should be easy to update with new content.	
EGOV/FR/1.29	Design and Construction: - Work closely with the RMC at each stage of the design to identify user needs and corresponding user interface requirements, workflows, and functionalities. - Ensure integration of all elements including content, information format, compatibility with software platforms used by RMC and standards for content management. - Select a platform that allows easy integration of multimedia products and user-friendly administrator interface. - Create wireframes, storyboards and prototypes to propose options for implementation. Provide three (3) template designs for review in order to select a concept. Concepts should reflect the RMC's corporate identity, nature and purpose.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Develop corresponding user interface components (web templates, style sheets, scripts, images, dashboards, social media interfaces) as needed. - Use simple, cost-effective techniques to test designs with representatives of target audience prior to launch of site. - Submit the final concept to RMC for review prior to 'going live.' - Secure the existing website prior to transitioning to the new platform. - Keep a full backup of the website through the duration of the project. - RMC will own and host the new site design and will be provided with a full backup copy of the site design and code at the closing of the project. - Content Migration - The complete migration of the new website to existing RMC URL. Deployment of new content.	
2. Citizen Portal		
EGOV/FR/2.1	It shall be a state of the art portal.	
EGOV/FR/2.2	At the core of the stakeholders service experience will be RMC portal which will be a gateway to various stakeholders including citizens, tourists and businesses. The Portal will have an intuitive user interface for rendering various services and providing role based access to various systems in use at RMC. Through the Portal, any user can seek service, status check on service request, lodge an incident/complaint, get information, and provide suggestions.	
EGOV/FR/2.3	The Face to face contact point for the citizens will be a Citizen Facilitation Centre. The Citizen Facilitation centre would be manned by trained employees of the RMC. These employees shall assist the citizens with information, application or complaints. The employees shall also take care of e-mail, postal service letters and phone calls. The employees shall log into the portal and conduct the business required for the citizen.	
EGOV/FR/2.4	The key objective of the Portal, Facilitation centre, Mobile App or the citizen centre will be to: - Provide Single Window services to citizens on anytime, anywhere basis - Provide a single and integrated view of RMC information system	
EGOV/FR/2.5	At each point, the process flow shall be through the portal.	
EGOV/FR/2.6	Broadly Portal is required to provide the following features - Role based access to core systems like GIS system and any other system - Link to E Government Services – Birth and Death certificate, Grievance redressal, Trade licenses, RTI, Legal case management, etc. - Management Reports and KPI Dashboard - Provision to request any service	
EGOV/FR/2.7	The portal would be accessed by: - General public & corporates - Citizen – residents - Tourists - Commercial establishments - Education establishment - Health establishment - RMC employees - Government - Third party vendor Each type of stakeholder shall have different needs and the portal will facilitate all requirements.	
EGOV/FR/2.8	The portal also needs to have mobile mirroring with Android, tablet & iPhone compatibility.	
EGOV/FR/2.9	Website, Citizen Portal and Mobile App shall be in English and Oriya and shall be user friendly.	
EGOV/FR/2.10	Website, Citizen Portal and Mobile App shall be single window service to	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	stakeholders with a single and integrated view of RMC and RSCL information system.	
EGOV/FR/2.11	Multi-user system with multi-level security system included.	
EGOV/FR/2.12	The various users shall be authenticated from the common LDAP server for which the roles will get assigned from the server. Depending on their roles and responsibilities, the respective users should be taken to their respective home page. The layer shall visually integrate the applications in place with single-sign-on implemented. LDAP roaming profile shall ensure seamless mobility of the user.	
EGOV/FR/2.13	Citizens who are residents: This shall give him access to his ledgers, digital locker and registering complaints. It shall also facilitate payment of utility bills. They can log in using a property id. In any of the cases, the basic data (including pending payments or dues) shall be populated for their viewing. The citizen can apply for certificates by clicking on the 'apply for certificates' link. This shall take the user to the e-Gov section for certificates. Similarly, the user may click on the RTI, Grievances or pay utility bills link by clicking 'apply for services'. It is expected that through one login one id, multiple departments can use common authenticated documents of a citizen from the respective citizen digital locker to provide services without the need of the citizen to provide same document to multiple departments within RMC. The citizen will need to interact with RMC for any of the following reasons (but not limited to): - Information - Consolidated application for utilities - Grievance / Complaints regarding municipal services - Primary education and medical needs (planned and maybe outsourced) - Allotment of Trade Licenses (direct or indirect) - Assessment & payment of taxes: Land related maintenance charges, and other government taxes as applicable - Utility Payment: Payments relating to electricity, water bills - Application & issue of Certificates - RTI All the above should be tiles on the landing page.	
EGOV/FR/2.14	Industrial units shall also have a section with a pre-decided format wherein they must upload key performance data every month or on a defined frequency. This will pertain to production, employment, tax paid, etc.	
EGOV/FR/2.15	Commercial establishments will have access to the data as citizens; with additions of links to the trade licenses of the e-Gov modules. They shall also have an MIS format to upload data for monthly MIS requirements.	
EGOV/FR/2.16	Education institutions will have access to data as above and in the future, will have a link from the portal for the citizen. They shall also upload MIS data such as (but not limited to): - Building self or rented and how much is area - Whether it has playground, lab facility, and library - Mid-day meals - Classrooms with infrastructure Electricity - Water supply - Toilet availability - Gender wise students in each class - Teachers in the school with details (TGT PGT etc. and), Educational qualification, permanent or contractual, number of years of experience - School dropout rates - Passing students percentage It is required to create log-in category for educational institutions and formats for periodic upload of this data and flag delays in upload of the same.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	Further, there may be a need to integrate advanced technology such as virtual classroom with the e-governance services of RMC. The technology infrastructure required at the school level for the remote classroom shall be provided by the respective education institute but the necessary integration with e-governance shall be a part of the Project.	
EGOV/FR/2.17	RMC employees shall have access to the portal with respect to their work requirement. They shall access e-Gov systems for all approval and reporting purposes based on the clearances inherent in the role and hierarchy. The portal may be accessed for registering a complaint, issuing a certificate, verifying status of projects, updating GIS databases and other work flow requirements.	
EGOV/FR/2.18	Any Outsourced employees: They shall have access to operation and maintenance functions as required. Events shall be triggered on application for utilities, initiation of projects or receipt of complaints and passed on to the concerned employees.	
EGOV/FR/2.19	RMC and Outsourced employees shall have access to e-Gov modules. They shall also have access to the detailed desktop and web version of the GIS map to be able to respond to the event and update the database.	
EGOV/FR/2.20	Through service Portal, any user can seek service, status check on service request, lodging incident/complaint, getting information, providing suggestions.	
EGOV/FR/2.21	Portal shall also be accessible in 3 languages – English, Hindi & Oriya	
EGOV/FR/2.22	Links: Links should be placed within the website to allow individuals to contact institutions affiliated with the RMC and RSCL and access to the portal as well the respective Ministries (can be called Useful Links).	
EGOV/FR/2.23	The user shall contact RSCL by following means: - In person through Citizen Facilitation Centre - Mobile Application - E-mail - Web Portal - Surface mail - Digital service kiosks In any of the above cases, the citizen query / data must interact with the e-Gov / Other system to be processed. It is expected that in any situation the query shall be directed to the portal and the data input by the citizen or the operator at the facilitation centre.	
EGOV/FR/2.24	Easy access to Key performance indicators: Seamless integration with RMC's and RSCL's dashboard data to provide continuously updated graphs and charts. This will be decided with RMC and RSCL input & consent.	
EGOV/FR/2.25	Downloadable resources: Provides a resource section with links to downloadable documents and templates appropriate to the audiences.	
EGOV/FR/2.26	News/Update feed: Constant and dynamic update feed on site home page. Displays announcements and notifications for new content additions on front page of site.	
EGOV/FR/2.27	Calendar: A dynamic calendar that displays events as well as filters for searching/sorting events.	
EGOV/FR/2.28	Users-Only Content: Certain content will be available ONLY to authenticated users. Account creation is limited to site administrators. User password recovery and profile management functionality is required.	
EGOV/FR/2.29	Contact Form: Provides a web-based contact form with anti-spam controls.	
EGOV/FR/2.30	Social Media Engagement Tools: New tools to improve interaction with social media	
EGOV/FR/2.31	Blog: The site should have a Blog section to facilitate discussions on various topics.	
EGOV/FR/2.32	Career: The site should have a career section which should accept online job application that would be fed directly into the HRM system.	
EGOV/FR/2.33	Language Options: The website ought to be easily translated into other languages even if documents remain in English.	
EGOV/FR/2.34	Compatibility: Site must be compatible with Google Chrome, Microsoft® Internet Explorer 8.0 or higher, Microsoft Edge, Mozilla Firefox, and Safari 5.0 or higher.	
EGOV/FR/2.35	Mobile Access: Site must be "responsively designed" to accommodate mobile users. This must include accommodations for slower, cellular internet connections. This includes compatibility with iOS, Android and other industry standard platforms.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/2.36	Settings: Website must not require plug-ins as a default.	
EGOV/FR/2.37	Performance: Site must be able to handle multimedia (video) with high performance.	
EGOV/FR/2.38	Web Metrics: Must be able to have a wide range of web analytics functionality that can track and analyse how people use the website and produce meaningful reports.	
EGOV/FR/2.39	HTML Compliance: Full compliance with HTML 5.0 or higher.	
EGOV/FR/2.40	Content Migration: MSI will transfer existing content into the new site template.	
EGOV/FR/2.41	Parallel sites: After 'Go Live' there should be two (2) sites running parallel, one for testing purposes and the other for production. All maintenance should be carried out in the test environment and be approved before migrating to the live environment.	
EGOV/FR/2.42	Easy Maintenance: Site should be easy to maintain, site should not require significant investment of time to keep site up and working with quick and easy fixes site should be easy to update with new content.	
EGOV/FR/2.43	The Portal platform should support deployment on all three platforms - Linux, UNIX and Windows.	
EGOV/FR/2.44	The Portal platform should provide support for portal standards such as JSR 168, WSRP 2.0 and JSR-170	
EGOV/FR/2.45	Ability to provide single information view of the data coming from multiple sources such as web service, XML, SQL source, Web Pages and Spreadsheets.	
EGOV/FR/2.46	Should support Class II/Class III Digital Signature Certificate for Login, Signing & Encrypting massages & attachments.	
EGOV/FR/2.47	Support for centralized, web based user provisioning ensuring single definition of users, roles, groups and access rights.	
EGOV/FR/2.48	System shall have search capabilities that support powerful and comprehensive full-text searching, metadata searching or people search.	
EGOV/FR/2.49	It should support multiple databases like Oracle, SQL Server, DB2, Informix etc. without requirement of any additional software.	
EGOV/FR/2.50	Should be able to manage portal content using web content management from common content management repository through out-of-the-box integration.	
EGOV/FR/2.51	The portal solution should allow the users themselves to personalize their user interface.	
EGOV/FR/2.52	The portal solution should provide several layers of caching infrastructure to provide content to users. Access to content should be cached to reduce the load and increase performance.	
EGOV/FR/2.53	Portal should support a stand-alone, service-oriented architecture.	
EGOV/FR/2.54	Support for out of the box integration with content management system for web content management and publishing on the portal.	
EGOV/FR/2.55	Support for unified Single Sign On for internal integrated applications	
EGOV/FR/2.56	Support for personalization of home page using drag & drop functionality	
EGOV/FR/2.57	Support for personalized notifications and alerts	
EGOV/FR/2.58	The portal solution should provide analytics console for accessing portal metrics. The analytics console should be available as an integrated application so that the product is easy to learn and easy to deploy.	
EGOV/FR/2.59	The portal solution should provide secure and controlled access to the analytics console. Only portal administrators should be able to access the console without exposing data that might be sensitive or private.	
EGOV/FR/2.60	Portal should provide comprehensive tracking and graphical display of portal/community traffic, searched keywords, quick system response time (less than 1 sec on landing page), document downloads, user turnover, visit duration, etc.	
EGOV/FR/2.61	Portal should provide a next generation Web 2.0 portal framework built specifically for Web 2.0 services like wikis, blogs and other Collaboration functionalities like Communities	
EGOV/FR/2.62	Support for linking, tagging and RSS feeds	
EGOV/FR/2.63	Support for discussion forums	
EGOV/FR/2.64	Supports a single, integrated, best of breed development environment to enable consistent design time and run time environment.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/2.65	Leverages a common management console to manage all distinct applications/modules and also monitor performance.	
EGOV/FR/2.66	Provides ability to perform Advanced Search based on multiple metadata	
EGOV/FR/2.67	Supports secure crawling of the content sources and perform indexing	
EGOV/FR/2.68	Support for parallel querying to improve search query performance	
EGOV/FR/2.69	Search results are based on user's security role and display what the user is authorized to access.	
EGOV/FR/2.70	Ability to integrate with LDAP based security.	
EGOV/FR/2.71	Support for analytics on Search performed such as reports on most popular searches, documents not found etc. Based on this administrator can boost document relevancy and customize search results.	
EGOV/FR/2.72	Support for embedding Search as a Service so that searches can be invoked via Service API. Search facility should provide suggest facility	
EGOV/FR/2.73	It should provide rapid application development tool for designing the framework along with debugging facilities. This development tool should support server based implementation.	
EGOV/FR/2.74	Portal should provide Template driven portal development to simplify portal creation process	
EGOV/FR/2.75	The portal should implement security features, such as password complexity, automatic blocking (temporary/permanent) of user logins after given number of unsuccessful login attempts (should be parameterized), controlled access to content stored on the portal and logging of security incidents using Identity management solution.	
EGOV/FR/2.76	Reporting and Monitoring should be inbuilt and provided as part of Portal inherent capability.	
EGOV/FR/2.77	Inherent Portal analytics should be able to capture page traffic, portlet traffic, content usage, services and response times.	
EGOV/FR/2.78	Analytics console with inbuilt UI framework for Analytics reports, graphs and charts.	
EGOV/FR/2.79	Should support a single content management repository for both structured and unstructured content.	
3. Birth & Death Certificate Module		
EGOV/FR/3.1	Birth & Death Certificate Module shall have the functionality of offering following services: - Birth Certificate Application Request - Birth Certificate Application Status - Online payment for Birth certificate - Birth Certificate Printing - Birth Certificate Search - Birth Statistics - Death Certificate Application Request - Death Certificate Application Status - Online payment for Death certificate - Death Certificate Printing - Death Certificate Search - Death Statistics - Birth/ Death Certificate Modification Request	
EGOV/FR/3.2	It shall be a Web based Scalable solution	
EGOV/FR/3.3	It shall have Secured authentication and authorization mechanism to enable internet access	
EGOV/FR/3.4	It shall have Scalable architecture framework for tech enabling plug and play solutions.	
General Registration Requirement		
EGOV/FR/3.5	Portal shall have information about the Birth / Death processes & documents required for the convenience of the citizen	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/3.6	System shall have facility to avail the service online & through CFC.	
EGOV/FR/3.7	System shall capture all the details and documents required for application	
EGOV/FR/3.8	System shall have facility to download required forms. System shall have provision for e-forms	
EGOV/FR/3.9	System shall have facility for online payment and through CFC.	
EGOV/FR/3.10	System shall have facility to send the alerts through SMS and email.	
EGOV/FR/3.11	System shall have facility to accept the request for certificate to be sent through courier/mail. For this system shall capture the address at which the certificate needs to be delivered and charges should be calculated accordingly.	
EGOV/FR/3.12	System shall have the facility to deliver the issued certificate via mail by official to the applicant.	
EGOV/FR/3.13	System shall have the provision to maintain Birth Register as defined in the process.	
EGOV/FR/3.14	System shall have the provision to maintain Death Register as defined in the process.	
Registration of Birth/Death:		
EGOV/FR/3.15	System shall provide an interface to hospitals/ individual for online registration of birth/death. Alternatively, same shall be done by CFC official using the similar interface once the information is received by the CFC official.	
EGOV/FR/3.16	The system shall follow due diligence to authenticate the identity of the applicant and the authority to apply and receive the certificate.	
Data to be captured:		
EGOV/FR/3.17	Registration of Birth (Hospital / Home / Jail / etc.) - Normal & Delayed Registration - Child Details – Gender, DOB, Time, Weight, Name, Birth Place, Birth Mark etc. - Parent Details – Name, Address, Qualification, Occupation - Delivery Method, Informant Details, Attachments in case of delayed registrations - Registration of Still Birth - Foetal Death Cause along with other birth registration details - GIS (for marking the hospital + parents address)	
EGOV/FR/3.18	Registration of Death - Name and address - Normal & Delayed Registration - General Details – Gender, DOD, Time, Name, Attention type, Pregnancy related Death - General Details –Death place type, death place, Cemetery type, Informants Details - Medical Certificate Details - Death Cause, Death Manner	
EGOV/FR/3.19	Defining charges For Birth and Death Services - Delay Charges based on no. of days of delay - Birth Certificate charges - Death Certificate charges - Child Name Insertion charges - Duplicate certificate charges	
EGOV/FR/3.20	Integration with Web to validate the Birth / Death Certificate	
EGOV/FR/3.21	Generation of birth and death certificates with provision of using digital signature and barcodes	
EGOV/FR/3.22	Online facility for new hospitals to apply for registration to use the system	
EGOV/FR/3.23	Integration to citizen and KPI database for updation and reflection in statistics.	
Name Corrections in Birth/Death Certificates:		
EGOV/FR/3.24	Govt. official shall be able to add/modify/delete the Birth and Death details based on the approval/right as per process.	
EGOV/FR/3.25	System shall have the facility to upload additional documents required.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
Late Registration of Birth/Death:		
EGOV/FR/3.26	System shall have the facility to allow the late registration of birth/death as per the rules.	
EGOV/FR/3.27	Application shall be automatically routed to the concerned Govt. Officials as per the duration gap of the registration as per the Birth/Death registration rule.	
EGOV/FR/3.28	Name Entry for Birth Registration	
MIS:		
EGOV/FR/3.29	Variety of Reports to be sent to State / Central govt. authority	
EGOV/FR/3.30	Monthly Summary Report of Birth	
EGOV/FR/3.31	Monthly Summary Report of Still Birth	
EGOV/FR/3.32	Monthly Summary Report of Death	
EGOV/FR/3.33	Birth / Death reports for various Health Schemes	
EGOV/FR/3.34	Reports to Health Department w.r.t. Death Causes in a particular period	
EGOV/FR/3.35	Reports to analyse services delivered through various delivery channels	
EGOV/FR/3.36	Birth Reports by Education of Father and Mother	
EGOV/FR/3.37	Birth Reports by Occupation of Father and Mother	
EGOV/FR/3.38	Birth Reports by Age of Mother	
EGOV/FR/3.39	Birth Reports by Sex and Month of Occurrence	
EGOV/FR/3.40	Birth Reports by Hospitals wise Counts	
EGOV/FR/3.41	Birth Reports by Sex ratios wise	
EGOV/FR/3.42	Child Mortality Report	
EGOV/FR/3.43	Report on Institutional Deaths	
EGOV/FR/3.44	Other periodic reports	
4. Trade Licensing		
EGOV/FR/4.1	This module shall have a linkage to the property tax module for appropriate tax assessment.	
EGOV/FR/4.2	Service Objective: Permitting business units to trade	
EGOV/FR/4.3	Stakeholders: Citizen, Data Entry Operator, Marketing Inspector, Office Secretary, Dealing Assistant, Tax Collector, CEO	
EGOV/FR/4.4	Process Input: Declaration Form	
EGOV/FR/4.5	Process Output: Trade License	
EGOV/FR/4.6	Integration Requirements: SMS Gateway, Payment Gateway, GIS, Property tax, Utilities	
EGOV/FR/4.7	Services: License application, License Online Receipt Print, License Online Receipt Search, License Renewal	
EGOV/FR/4.8	Configuration - Business types - This includes the configuration of different business licenses. - Business Categories – This includes the configuration of business categories like Whole seller, retailer, manufacturer etc.	
EGOV/FR/4.9	Master Data: - Business owner types - Holidays - Products - License Types - License Groups - Licenses - Required Licenses - Business Rules - Product Usages - Product Permissions - License Reports - Signing Authority	
Information in the Master:		

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/4.10	Sanitary zone/division information in the Sanitary Zones/wards/Division Master	
EGOV/FR/4.11	In the Revenue Master: - Revenue wards information under sanitary zones/wards/divisions - Revenue blocks under revenue wards information.	
EGOV/FR/4.12	Election Wards Information	
EGOV/FR/4.13	Locality categories	
EGOV/FR/4.14	Sanitary zones/ward/division allocation to Sanitary Inspectors (SI)	
EGOV/FR/4.15	Trade categories	
EGOV/FR/4.16	Sub-trade categories	
EGOV/FR/4.17	Allow the configuration of: - Late fee details for the corresponding time periods in the penalty fee master - Trade rates - Revenue Block Categorizations	
EGOV/FR/4.18	Details of an applicant for a new trade license.	
EGOV/FR/4.19	Preparation of report of field inspection of the applicant's premises	
EGOV/FR/4.20	Recording the NOC/Installation Permission Details.	
EGOV/FR/4.21	Allow the Municipal Commissioner to view the recommendations of the SI/HO on a new license application.	
EGOV/FR/4.22	Facilitate the Commissioner to enter his remarks in the above case	
EGOV/FR/4.23	Capturing of the license fee/late fee details (Cheque/DD details, etc.)	
EGOV/FR/4.24	Generation of a new license after the information on the necessary approvals are recorded in the system.	
EGOV/FR/4.25	Allow printing of the license document from the system.	
EGOV/FR/4.26	Recording the application details from the application form submitted by the applicant.	
EGOV/FR/4.27	Data from the application collected for License renewal	
EGOV/FR/4.28	Recording of the trade License renewal details	
EGOV/FR/4.29	Recording of the Panchanama details collected from the SI reports	
EGOV/FR/4.30	Generation of the list of defaulters of renewal fees	
EGOV/FR/4.31	Generation of the list of license holders who wish to close their trades on their own	
EGOV/FR/4.32	Update the status of a trade license as 'active' or 'closed', and the reasons for closure are entered	
EGOV/FR/4.33	Recording of the details from the application submitted by the applicant for change of Title	
EGOV/FR/4.34	Generation of license with changed title, after necessary steps completed	
EGOV/FR/4.35	Allow printing of the above license	
EGOV/FR/4.36	Details of the un-assessed trades-individuals performing trade without a proper trade license	
EGOV/FR/4.37	Track the renewal notices sent to the license holders to renew their License.	
EGOV/FR/4.38	Track response dates, late fee applicability, etc. for the above	
EGOV/FR/4.39	Capture of grievances against a license, or in general.	
EGOV/FR/4.40	Generation of demand collection and balances revenue ward-wise for the ULB	
EGOV/FR/4.41	Processes - Issue of new license - Duplicate License - Registration of Application. - Verification of Application - Status check of application - Automatic alert for license renewal - License issue or rejection of the application - Renewal/Closure of license - Change in Name of Business - Change in Business - Transfer of License	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Issuing the demand notice to the license holder for renewal of his trade license. Depending upon the timeliness of the payment of the license renewal fee, the license is either renewed or a closure notice is issued to the licensee. - Cancellation of License	
EGOV/FR/4.42	Workflow - Capture of License Details - License Holder's Details – One or multiple owners - Capture of Mobile No. / E-Mail ID - License holder's photograph(s) - Link to Property Number - License Details – Temporary/ Permanent License, Name of Business, Business Address, - Trade/ Business Details – License Type, Subtype - multiple levels to define types and sub types. - License type, sub-type, unit of measure wise license amount.	
EGOV/FR/4.43	Issuance of License - License Application - Calculation of License Fee - Online payment of license fees - License Online Receipt Print - License Online Receipt Search - Letter of Intent - License Certificate - License Renewal	
EGOV/FR/4.44	License Sanction Process - Applicant Entry - Business Information Feeding and application number allocation. - Authenticate the application before registering it. - Receipt for issuing license. - Authenticate the application by the authority. - Sanction/Renewal of license - Rejection of license - Cancellation of application - Log Management of the issuing/renewal of licenses - Automatic/Manual Surcharge Calculation - Automatic Renewal of licenses on receipt but should be authorized by the authority.	
EGOV/FR/4.45	Other departmental process: - Scrutiny of Applications - Inspection Entry - Generation of Show cause Notice Hearing - Reminder Notice for Renewal - Cancellation of License by Force	
EGOV/FR/4.46	Search facility - For the issued licenses - Renewal of licenses - Pending Applications	
EGOV/FR/4.47	The reports (at least): - Different types of licenses - Pending Application Report	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Expiry License Reports - Renewal License Reports - Notices for the renewal of licenses - Applicant List - Issued Card List - License Income Report - License status/log report	
EGOV/FR/4.48	Integration with other Modules - Finance module: - automatic posting of the receipt amount to the cash ledger and license ledger. Automatic renewal of the license on receipt. - SMS / email integration - GIS - Property tax - Utilities - Payment Gateway	
EGOV/FR/4.49	MIS - License Register - List of Defaulters - Reminder Notice for Renewal - Demand / Collection Register - Reports showing Changes in License Types, Business Partners, Cancellation Licenses, etc. - Facility to forecast the impact of reduction / deduction of License Fee	
5. Right to Information (RTI)		
EGOV/FR/5.1	RTI module shall provide all services under RTI under a single category	
EGOV/FR/5.2	RTI module shall be able to retrieve service request form	
EGOV/FR/5.3	RTI module shall be able to route the service request to concerned officer (Public Information Officer - PIO)	
EGOV/FR/5.4	RTI module shall have the functionality to accept service request even if the service request is not directed to particular section	
EGOV/FR/5.5	RTI module shall be able to route such application to CEOs' office for further re-routing	
EGOV/FR/5.6	RTI module shall allow CEO to allocate service request to concerned PIO for service request under "other categories"	
EGOV/FR/5.7	RTI module shall auto generate notification of pending service delivery request to concerned PIO on successful submission of service request	
EGOV/FR/5.8	RTI module shall be able to send SMS alert/Auto generated mails to the applicant and concerned authorities whenever required	
EGOV/FR/5.9	RTI module shall allow the concerned PIO to accept / reject the service request as per the guidelines of the RTI act	
EGOV/FR/5.10	RTI module shall in case of rejection, the system should allow the concerned PIO to state the reason of rejection	
EGOV/FR/5.11	RTI module shall in case of acceptance, the system should open a new page with all the accepted service request by the concerned PIO	
EGOV/FR/5.12	RTI module shall allow the PIO to send mail with a format of Form B and Form C	
EGOV/FR/5.13	RTI module shall save the acceptance / rejection only on digital signature of the PIO	
EGOV/FR/5.14	RTI module shall auto generate notification to concerned officials about service request allocation	
EGOV/FR/5.15	The system should display content about RTI & RTI circulars. It should also display: - Names of PIO - Details of Departments: Introduction, Objectives, responsibilities, powers & duties of officers, employees with gross salary, activities, time limit,	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Directory with telephone numbers. - Committee: Members, purpose, type, freq. of meeting, docs available for public. - Projects/ Activities: Budget head, work activities, allocated amount, current statistics. - Details of concessions, subsidies given, computerization done in various depts. - Integration required for updation of data for RTI with projects, accounts, HRMS, Fleet, material, asset. - Scope as per RTI Act	
EGOV/FR/5.16	Request shall be received on the portal, the mobile application or at the citizen facilitation centre. The request shall be forwarded appropriately and track kept of the information supplied and time lines. The request shall also be forwarded from the state government or information commission. In each case the information supplied has to follow the same path.	
EGOV/FR/5.17	Display details of PIO, Department official's details with contact, RTI circulars, scope as per RTI Act, etc.	
EGOV/FR/5.18	MIS information shall include: - Number of RTI filed - Pending RTI - Department / Employees involved - RTIs closed	
6. Legal		
EGOV/FR/6.1	RMC shall decide what information shall be posted on the dashboard. It should also link to the customer master (using property id) for any transaction / interaction / case for updation of current situation.	
EGOV/FR/6.2	Creation of master database of all cases (Both pending & closed cases) & empanelled advocates.	
EGOV/FR/6.3	Linking of project, branches & user with case master.	
EGOV/FR/6.4	Provision for registering new cases.	
EGOV/FR/6.5	Categorization of cases as per the nature.	
EGOV/FR/6.6	Provision to forward the cases to empanelled advocate.	
EGOV/FR/6.7	Provision for uploading case related document.	
EGOV/FR/6.8	Creation of Para-wise-comment (PWC) by branches those are tagged to that particular case and sending it to legal section of RDA.	
EGOV/FR/6.9	Consolidation of all the PWC and sending it to the respective empanelled advocate.	
EGOV/FR/6.10	Preparation of counter affidavit by empanelled advocate on basis of PWC collected.	
EGOV/FR/6.11	Provision for updating case status through the module.	
EGOV/FR/6.12	Monitoring of the case result.	
EGOV/FR/6.13	Provision of advance search option to track the case details. Search option should have provision to search any case by name / case number /mauza number / year etc.	
EGOV/FR/6.14	Provision to check the status of particular case of RDA in ODA court or any higher court.	
EGOV/FR/6.15	Integration with payment gateway to make case related payments.	
EGOV/FR/6.16	Integration with File Tracking Application.	
Master		
EGOV/FR/6.17	Advocates, Law firms & their fees	
EGOV/FR/6.18	Court Master	
Case Management		
EGOV/FR/6.19	Registration of new cases, allocate advocate, allocate RMC officer	
EGOV/FR/6.20	Facility to attach various documents related to the case	
EGOV/FR/6.21	Entry of Date of Hearing	
EGOV/FR/6.22	Alerts to officers w.r.t. hearing date	
EGOV/FR/6.23	Entry of hearing details	
EGOV/FR/6.24	Capture of judgment	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/6.25	Details of payments to the advocates & law firms	
EGOV/FR/6.26	Linkage to the departmental data	
EGOV/FR/6.27	Linkage to GIS to capture location reference for cases	
EGOV/FR/6.28	Legal Opinion on various departmental queries, agreement Formats to be stored in Document Management Module	
MIS		
EGOV/FR/6.29	Case Pendency reports (Department-wise / advocate or law firm wise / Officer-wise)	
EGOV/FR/6.30	Reports w.r.t. Cases won / Lost / Appeals made	
EGOV/FR/6.31	Payments to the Legal Advisor / Law firms	
EGOV/FR/6.32	Repository for various act and provision with search option	
EGOV/FR/6.33	Integration / Link to Odisha Government site for references	
EGOV/FR/6.34	Repository of all the cases since 1950 by High court and Supreme Court with search feature.	
7. Welfare Schemes		
EGOV/FR/7.1	Master Entry of the different Schemes - AIDS awareness - Family planning and MCH - School health program - Janani Suraksha Yojana - Jeevan Dayi Yojana - RCH programs - Self-employment slum / Non slum - Training schemes - Education - S.S.C. & H.S.C. scholarship schemes - Contributory Health schemes - ICDS immunization programs - Integrated child development project - Any other Schemes	
EGOV/FR/7.2	Creation of Database of beneficiaries	
EGOV/FR/7.3	Recording and accounting of the grants / funds received for implementation of various schemes	
EGOV/FR/7.4	Preparing of the budgets for the implementation of the schemes	
EGOV/FR/7.5	Allocation of work and fund required for implementation	
EGOV/FR/7.6	Recording and accounting for the expenditure incurred for the implementation of the project	
EGOV/FR/7.7	Generation of necessary reports needed to monitor the implementation of the schemes	
8. Marriage Registration		
EGOV/FR/8.1	MSI may explore Aadhaar linked verification at the time of online application	
EGOV/FR/8.2	Multi-lingual support (English, Hindi and Oriya)	
EGOV/FR/8.3	Module will include: - Application for Marriage Registration - Application for Marriage Certificate - Online payment of registration fees - Provision to capture picture of bride and groom - Capture biometric finger prints - One level approval for the registration - Document verification - Signing of the certificate - Email delivery of digitally signed certificate	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Correction in Marriage Certificate - Application for Re-marriage	
9. Visitor Management		
EGOV/FR/9.1	This module is to be developed and implemented in all 3 stakeholder organisations.	
EGOV/FR/9.2	Registration of the visitors (personal details, contact details, purpose of visit, whom to meet, etc.)	
EGOV/FR/9.3	Capturing the in time and out time of the visitor.	
EGOV/FR/9.4	Integration with web cam and printer	
EGOV/FR/9.5	Generate reports as required	
10. Secretarial & Meeting Schedule		
EGOV/FR/10.1	This module is to be developed and implemented in all 3 stakeholder organizations.	
EGOV/FR/10.2	Maintain records of committees and members	
EGOV/FR/10.3	Proposal by various members to include topics in Agenda	
EGOV/FR/10.4	Preparation of Agenda for the meeting	
EGOV/FR/10.5	Preparing and printing Notice for the meeting	
EGOV/FR/10.6	Emailing the Notice to members	
EGOV/FR/10.7	Record the resolutions passed	
EGOV/FR/10.8	Preparation of Minutes of the Meeting and circulating the same	
EGOV/FR/10.9	Mapping and naming of the meeting rooms.	
EGOV/FR/10.10	Provision for checking availability of meeting rooms.	
EGOV/FR/10.11	Book/Schedule a meeting at an office for a desired location	
EGOV/FR/10.12	Tagging the officer / group with the respective meeting.	
EGOV/FR/10.13	Provision for preparation of agenda as per the organization standards.	
EGOV/FR/10.14	Tracking of agenda as per target date, assigned officer with status.	
EGOV/FR/10.15	Provision to upload the signed agenda in the system.	
EGOV/FR/10.16	Facilitate SMS notifications to participants and observers.	
EGOV/FR/10.17	Provision for intimating about the meeting to a particular user / group.	
EGOV/FR/10.18	Integration with Microsoft exchange server to push meeting details directly to recipient's outlook calendar.	
EGOV/FR/10.19	Tracking of Minutes of Meeting.	
EGOV/FR/10.20	Provision for assignment of tasks by MOM Controller as per the meeting decisions.	
EGOV/FR/10.21	Maintaining attendance records and drafting agendas, reports &minutes of meetings.	
EGOV/FR/10.22	Regular notifications to defaulters.	
EGOV/FR/10.23	All meetings to be broadly categorized like "Advisory Council Meeting", "Authority Meeting", "DP&BP Committee meeting" etc.	
EGOV/FR/10.24	If any meeting or any item of a meeting is related to any project of RDA / RMC / RSCL, then the project name should be tagged to that meeting/specific item, so that all decisions taken in different meetings relating to a specific projects can be fetched instantly.	
EGOV/FR/10.25	Provision for maintaining contact details with email ID, mobile No. etc. of both internal and external participants / members along with meeting hall in charge.	
EGOV/FR/10.26	While sending SMS to participants regarding the meeting scheduled, SMS also to be sent to meeting hall in charge to make necessary arrangements.	
EGOV/FR/10.27	Provision for distributing the agenda notes & MOM, etc. to all participants through email and sending an SMS regarding the same.	
EGOV/FR/10.28	As per MOM, target date provision to be kept along with task assigned to the officers and there should be provision for updating action taken report by them along with uploading of supporting documents if required.	
EGOV/FR/10.29	Provision for uploading scan copy of agenda notes and proceedings with minimum metadata like meeting date, subject, name of participants etc. for old authority meetings, advisory council meetings, etc.	
EGOV/FR/10.30	Generation of officer-wise action taken/action pending report for particular or all meetings conducted during a date range.	
EGOV/FR/10.31	SMS alerts to concerned officer on target date for non-compliance of tasks.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
11. NOC		
EGOV/FR/11.1	This module is to be developed and implemented in all 3 stakeholder organizations.	
EGOV/FR/11.2	The application should support setting up various services for issues NOCs by the organization.	
EGOV/FR/11.3	Creation and categorization of NOC as per the requirement.	
EGOV/FR/11.4	Defining fees for different kind of NOCs	
EGOV/FR/11.5	Defining pre-requisites, mandatory documents for each NOC	
EGOV/FR/11.6	Provision to apply online for NOC through the system.	
EGOV/FR/11.7	Facility to upload the scanned attachments	
EGOV/FR/11.8	Online payment of fees by the Citizen/ applicant	
EGOV/FR/11.9	Defining the approval hierarchy.	
EGOV/FR/11.10	Tagging of timeline for each level of approval.	
EGOV/FR/11.11	Directing it to the respective branch for approval.	
EGOV/FR/11.12	Issuance of NOC through system.	
EGOV/FR/11.13	SMS and email notification to the applicant once the NOC is approved	
12. Building Plan Approval		
EGOV/FR/12.1	The Building plan Approval with Common Application Form is an E-Governance Project to be developed by MSI.	
EGOV/FR/12.2	This module must update the property master for appropriate tax assessment.	
EGOV/FR/12.3	Broad Functionality includes - Issuance of Commencement Certificate by applying through Common Application Form - Issuance of Occupancy Certificate - Issue of Certified Copy of Building Plan Approval - Empanelment of Technical Person - Renewal of Empanelment - De-listing of Empanelled Technical Person - Application View Interface to external agencies to add comments, process NOC.	
EGOV/FR/12.4	The entire application is broadly classified into four major sections - Client/Citizen Portal - Common Application Form - Building Plan Approval System - Citizen Delivery System	
EGOV/FR/12.5	Client/Citizen portal is the external interface where citizen and technical person are registered as a user to access the CAF application.	
EGOV/FR/12.6	Department users from RMC, RDA and external public agencies can access the CAF through Building Plan Approval system. Department users validates the documents as per the checklist based on project category, perform joint site inspection, if any discrepancies found during the process email or SMS notification sent to the citizen or technical person for re submission of application and supporting documents.	
EGOV/FR/12.7	External public agencies after site visit can put objection and provide comments to comply as per rules or can grant NOC for the same.	
EGOV/FR/12.8	Citizen Delivery system consists of all the MIS reports like site inspection report, employee turnaround time which are being used for departmental decisions.	
EGOV/FR/12.9	Once the building plan is approved the system should be integrated with Property Tax module of RMC to send alerts to other stakeholders/ system/ relevant services provided by the Urban Local bodies.	
EGOV/FR/12.10	Key Features of client Portal - Technical person registration - Apply for Building plan approval using Common Application Form - Track status of application online	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Apply for occupancy certificate	
EGOV/FR/12.11	Key Features of BPAS main portal - Add Noting, Site Inspection notice, forward to next level. - Should have provision to auto-detect of structures based on usage such as e.g. Residential, Commercial or Residential- Commercial Mixed usages) and also detect high-rise and non-high raised category of buildings - Auto generation of building parameters like Setbacks, FAR, coverage, built up area, building heights etc. - Auto-generation of plot area statement (length, width, total area)for cross verification with system entered value by triangulation - Should have provision to enable auto detection of side margins and verification of coverage area. - Auto-Triangulation: Should have provision to generate Plot area Diagram by Triangulation Method & Plot Area calculation itself for cross verification. - Auto-Dimensioning with Block Diagram: Should have provision to generate Block diagram for each Floor and provide dimensions with Area Calculation. - Should have provision to automatically insert Schedule of Opening for each Building. Same way inserts Proposed Parking for whole Project. - Margin Generation: Should have provision to generate required Margin from Main Road, Plot Boundary, Open Space etc. itself. Even it should show Proposed Failed Margin with Auto Dimensioning. - System should have provision to accept NOC from different external agencies like Fire, PH, NAI, NHAI, Department of Forest & environment/ State Environment Impact Assessment Authority (SCIAA), Archaeology Survey Of India (ASI)/ Odisha State Archaeology, Traffic, Police etc. and process the application accordingly. - Generation of Scrutiny Reports: It should have provision to generate the various scrutiny reports dynamically based on the Rules described by the Authority. Generated report shows the Failed/Passed Items with their rules in a very user friendly Viewable/Printable format. Customization of Reports can be made using user defined templates. Software reads the building entities from drawings, geometrically map each & every entity by corresponding with complex & interlinked rules. After scanning and saving the drawing, scrutiny reports are generated where all failed and passed rules are displayed with required/permissible values with proposed values so that architect can easily correct them. - The system should automatically generate an SMS should be sent to the Architect and concerned Field staff if there are any cancellations of site visit, the system should intimate the key relevant people so as to avoid unnecessary wastage of time. Reasons for such cancellation should also be recorded in the system. - The system should generate MIS to be sent to higher authorities for approval and to make the approval status available online. - System generated building plan approval certificate	
13. Housing Scheme Management		
EGOV/FR/13.1	Definition of scheme master.	
EGOV/FR/13.2	Provision to upload the PPR (Pre Project Report) prepared for the respective scheme.	
EGOV/FR/13.3	Integration with meeting schedule for conducting a meeting regarding the scheme.	
EGOV/FR/13.4	Defining approval hierarchy for the same.	
EGOV/FR/13.5	Registration of beneficiaries identified for the scheme under this module.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/13.6	Database creation for the beneficiaries of this particular scheme.	
EGOV/FR/13.7	Authentication of beneficiaries through Aadhar card.	
EGOV/FR/13.8	House Allotment to the beneficiaries.	
EGOV/FR/13.9	Intimation to the beneficiaries through SMS/email.	
EGOV/FR/13.10	Definition of scheme master.	
14. Enforcement		
EGOV/FR/14.1	Requisition from RDA / other Government body / public for notifying RDA for any encroachment / unauthorized construction.	
EGOV/FR/14.2	Provision to receive the requisition by authority of enforcement department.	
EGOV/FR/14.3	Assigning central enforcement monitoring committee for verifying and authenticating the complaint and updating the status.	
EGOV/FR/14.4	Forwarding the case to ODA section for filing case against the opposition party.	
EGOV/FR/14.5	Provision to print “show cause” notice received by the ODA court for sending it to the opposition party.	
EGOV/FR/14.6	Updating the status of hearing for the same (Stay order / demolition)	
EGOV/FR/14.7	Defining the squad master and tagging the squad for demolition purpose.	
15. Land Acquisition, Land Bank of RDA and TDR		
EGOV/FR/15.1	Land Acquisition - Requisition to respective government body (RMC, tehsil, etc.) for acquiring the land that comes under their jurisdiction. - Provision to generate and print notice that will be sent to the respective citizen for acquisition of his / her land. - Provision for definition of land and GIS integration with land master data. - Submission of project proposal along with land detail. (Khata no., Plot no., Recorded tenant, location details, etc.) - Defining escalation mechanism for necessary approval. - Assigning sub-ordinate to carry out land acquisition activity. - Integration with “Bhulekh” for authenticating the details of the land. - Provision to upload field verification report. - Generation of public notice for grievance related queries. - Upload of grievance & resolution details. - Tracking of progress of the acquisition of land. - Provision of uploading physical possession details. - Generation of office order. - Intimation to the applicant through SMS / email.	
EGOV/FR/15.2	Land Bank of RDA - Integration with the land acquisition for getting the information of land acquired. - Database creation for all the land acquired or land already available with RDA. - Integration with GIS and Mapping of the land acquired. - Provision to add any further acquired land details. - Categorization and sub-categorization of the land by the help of which the RDA officials can search for any specific land. - Integration with GIS as per the business requirement of RDA. - Defining the categories of land such as residential, commercial, etc. - Provision to allocate the land to the respective entity in the specific category defined.	
EGOV/FR/15.3	Transfer of Development Rights (TDR) - Requisition for land to be acquired. - Identification and Registration of Beneficiaries for TDR. - Defining approval hierarchy for approval. - Document Submission, verification and authentication.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Verification of land. - Identification and allocation of land to the concerned person. - Provision for generation of TDR certificate. - Provision for tracking the status of application for TDR. - Provision to apply for renewal of TDR after five years for one time. - Provision to sale the TDR certificate to any other beneficiary.	
EGOV/FR/15.4	About Odisha Transferable Development Right (TDR) Rules The Odisha TDR Rules, 2015 has been notified by the State Government. This will facilitate the land owner to surrender the land affected by the amenities/infrastructure proposed in the Development Plan in exchange of development rights which can be utilized in the non- affected part of the plot or any other development rights may also be sold to anyone who wishes to construct beyond the applicable base FAR.	
16. Park Management System		
EGOV/FR/16.1	Defining the land for park.	
EGOV/FR/16.2	Geo-tagging of parks in the map	
EGOV/FR/16.3	Identifying different features of Park.	
EGOV/FR/16.4	Allocating budgets to the parks in accordance with respective feature.	
EGOV/FR/16.5	Monitoring of development and maintenance activity.	
17. Property Information Allotment System		
EGOV/FR/17.1	Functionality - Applicant Database - The citizens have to register themselves, Online through RDA website as per designed format. On registration a Unique-Account-No (UAN) will be assigned for future correspondence. - The online registration should have the provision of capturing / linking bio-metric data from UIDAI/AADHAAR number of all family members (above age of 5) at the time of registration - Allottee Database - The application so received will be first checked for any pre-existing property from the existing allottees from the Allottee Database - Validation of the Allottee Database - Advertisement and publications about a specific scheme - Applicants eligible for a particular Scheme will apply online - The brochure cost, application fee and EMD amount will be received online through e-Payment Gateway. - Processing of the Application as per Allotment Policy & Brochure Conditions. - Lottery (provision for IT – Randomization Technique)/ Manual Mode / Auction of properties and online intimation of drawls result through instant message (SMS) / email to the Allottees - Online - instant refund of the EMD amount to the bank accounts of the unsuccessful applicants through e-Payment gateway. - Instant Printing of Allotment Letters intimation through seed post as well as e-Dispatch system - Generation of Dues statement and online intimation – RULE Engine to be developed. - Auto generation of default notices and intimation - Auto generation of notice for determination of agreement. - Generation of Cancellation Notices as per brochure conditions. - Generation of Demand-Collection-Balance (DCB), Scheme wise – category-wise and allottee wise.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- MIS Reports - Payment and Receipt Database - All most all payments / Receipts should be online and posted to concerned ledger / account. - Provision may be kept for offline payments also as there are Allottees of EWS & LIG categories. - Online dues statement should be generated from the RDA website in order to enable Allottees to pay their dues timely and online.	
EGOV/FR/17.2	TRANSACTION MODULE - Online Application for issue of NOC / Tripartite-Agreement / Lease-Deed / Sale-Dead / Transfer of Properties/ Conversion / Mutation/Issue for permission for Mortgage/Conveyance Deed - Issue of the above orders.	
EGOV/FR/17.3	ESTATE AND PROPERTY MODULE - Property Database - Location and Area - Nos. and Category of Property developed - House No/Flat No/ Plot No/ Shop No/ Office Space No assigned with area of that particular property - Other relevant data about the property.	

EGOV/FR/17.4	User and Characteristics
	Following are the base layout of category of Users of PAIS Application and its Admin user
	This type of user is both Server and Application level user is responsible for
	- Creating necessary rules around the PAIS application
	- Creating various Master data Definition required for PAIS
	- Creating different users required to operate the system
	- Ensuring smooth day-to-day functioning of the server and manages the following configuration
	  - PAIS Middleware Service Application
	  - PAIS Server Configuration Application
	  - Integration Module of PAIS	

EGOV/FR/17.5	Functional User (Allotment Section, Finance Section, Engineering Section, Information Counter, MIS Section) This type of user is Application user and will have the privilege to access various application level functionality of PAIS - UAN Registration - Estate and Property Module - Allotment Process - Online and Offline Payment - MIS	
EGOV/FR/17.6	MIS User - This type of user is Application user and will have the privilege to access - Dash board featuring Key Performance Indicators, Alerts etc. - Special dashboard featuring Strategic Performance Indicators.	
EGOV/FR/17.7	Customer of RDA & Citizen This type of user will have the privilege to access various e-services provided by the RDA - To register for UAN - To apply online for Allotment of Asset, Transfer of Properties, NOC, Tripartite Agreement and Mutation etc. - To make online payment, which are outstanding against the allotment	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- To check the status of payments made till date. - To deal with RDA for any other transaction related to properties which are allotted	
18. Property & Holding Tax		
EGOV/FR/18.1	This module is currently being developed under NMMP program. Broad functionality is given below. Bidder shall make an assessment of the same and accordingly use, modify or replace the same.	
EGOV/FR/18.2	The system should have the following basic functionalities: - Online registration for property tax payments - Online Self-Assessment/ Calculation of Holding Tax by Citizens - Online payment of property tax - Facility to maintain the historical records of the properties (i.e. change of ownerships, usage, valuation etc.) - Interface for citizens to apply for transfer, separation and amalgamation of properties and subsequent adjustment to the tax-bills, if required - Facility to accept the objections against any valuation (proposed by ULB) and finalization of the same through a hearing process - Tracking and monitoring of defaulters and taking subsequent measures (e.g. issuance of 'Notice of Demand'/ 'Warrant Notice', seizure/action of property - Bulk generation of demand notices and sending of SMS/Email to property owners for tax payment - Generating various statistical reports	
EGOV/FR/18.3	The Revenue department handles the assessment of holdings and based on the assessment calculate the holding tax and generates the demand letter.	
EGOV/FR/18.4	The key requirements for Holding Tax assessment includes the following sub-modules: - Collection of Holding Tax - Self-Assessment/ Calculation of Holding Tax by Citizens - Updating Property Attribute Information by RMC/MSI Staff - Migration of Holding Tax Data	
EGOV/FR/18.5	Holding Tax has got the nomenclature of Property Tax in Orissa Municipal Corporation Act, 2003. As per Orissa Municipal Act, the Holding Tax is a percentage of annual value. It constitutes the prime source of Revenue for the Municipal Corporation. The tax assessment base for Holding Tax may be on (a) capital/commercial value basis or (b) rental value basis. Holding Tax is paid annually as per the announcement of the concerned Municipal Corporation/Municipality.	
EGOV/FR/18.6	All property tax rules should be configurable, to be changed as and when regulations are passed following required approval process.	
EGOV/FR/18.7	GIS Based property tax system covers the entire area of RMC jurisdiction and as a part of this system, a unique property tax identification number will be provided for each property. This unique identification number will be combination of ward number and plot number. GIS mapping of individual properties will bring un-assessed properties under the tax net. Satellite technology was used to measure the buildings, find out the nature of usage of the building, type of construction, number of floors and other related details.	
EGOV/FR/18.8	Geographic Information System solution consists of capturing, storing, editing, checking, integrating, manipulating, analysing and displaying geo-data related to positions on the Earth's surface and data related to attributes of the entities/holding tax payers in a ULB. Holding tax payer Indexing is defined here as a unique coding of index process for all types of holding tax payer into a data base structure, created with pre-determined attributes project area including locations with a facility using GIS tools to query and retrieve information. The holding tax payer indexing is essential for property tax database to maintain the system in a dynamic mode to	

<table>
<tr><th>S. No.</th><th>Minimum Functional Requirements</th><th>Compliant (Yes / No)</th></tr>
<tr><td></td><td>meet the day-to-day imperative changes.</td><td></td></tr>
<tr><td>EGOV/FR/18.9</td><td>The property data will have the Unique Identification Number generated from the new application which is a combination of Ward Number and Plot Number.</td><td></td></tr>
<tr><td>EGOV/FR/18.10</td><td>All spatial data will be supplied by H&UD department which will be migrated to the new system. The spatial data will be available in .shp format.</td><td></td></tr>
<tr><td>EGOV/FR/18.11</td><td>Any holding within Municipal Corporation limits having clear right, title, interest of the holder is liable to pay Holding Tax @ of 15% or 13% of the annual value of the holding depending on the wards:
<table>
<tr><th>Sl. No.</th><th>Name of Wards</th><th>Holding Tax</th><th>Light Tax</th><th>Drainage Tax</th><th>Total Rate of Tax to be collected on the ARV of Holdings</th></tr>
<tr><td>a.</td><td>4,5,7,8,9,28,29,30,32,33 & 4,15,16,17,18,19,20,21 & 22</td><td>10%</td><td>3%</td><td>2%</td><td>15%</td></tr>
<tr><td>b.</td><td>1,2,3,6 & 31</td><td>10%</td><td>3%</td><td>-</td><td>13%</td></tr>
</table></td><td></td></tr>
<tr><td>EGOV/FR/18.12</td><td>Government buildings, Government Hospitals, Government Educational Institutions, Government Cultural Institution only pay 5% or 3% towards latrine tax & drainage tax and such institutions are being exempted of paying 10% Holding Tax as per the Act.</td><td></td></tr>
<tr><td>EGOV/FR/18.13</td><td>In order to hold property within the jurisdiction of the Municipal area, the property holder has to pay Holding Tax as per the Act.</td><td></td></tr>
<tr><td>EGOV/FR/18.14</td><td>At the time of assessment /valuation if the ward supervisor / ward officer noticed that, there are buildings which are newly constructed. And till now they have not given the application for valuation of holding. For those building owners they will send the 1st Notice.</td><td></td></tr>
<tr><td>EGOV/FR/18.15</td><td>Even after first notice, if the concerned person is not responding then the 2nd Notice will be send.</td><td></td></tr>
<tr><td>EGOV/FR/18.16</td><td>Owner can submit the application directly without receiving any notice or even after receiving the notice.</td><td></td></tr>
<tr><td>EGOV/FR/18.17</td><td>Submission of application form</td><td></td></tr>
<tr><td>EGOV/FR/18.18</td><td>Once the valuation of the holding is done, next step is to send the notice of assessment where the tax details are mentioned.</td><td></td></tr>
<tr><td>EGOV/FR/18.19</td><td>No Application form is submitted: - Even after sending the 2nd notice also if the person is not submitting the application form, in this case, RMC suomoto does the valuation and sends the notice of assessment.</td><td></td></tr>
<tr><td>EGOV/FR/18.20</td><td>Based on the tax arrived in the notice of assessment RMC will send the demand notice.</td><td></td></tr>
<tr><td>EGOV/FR/18.21</td><td>Holding Tax Calculation</td><td></td></tr>
<tr><td>EGOV/FR/18.22</td><td>The amount of Holding Tax is different for Rental, Residential & Commercial purpose.</td><td></td></tr>
<tr><td>EGOV/FR/18.23</td><td>The Holding Tax Assessment procedure followed in RMC is mentioned below:
<table>
<tr><th colspan="2">(A) Residential Holding</th></tr>
<tr><td>Step I</td><td>Plinth Area of the holding in Sq. Meter * Rs.12.70 = say X</td></tr>
<tr><td>Step II</td><td>Deduct 15% of “X” towards repair and maintenance if the holding is more than 5 years old</td></tr>
<tr><td>Step III</td><td>Add 5% of the land cost where the holding is located</td></tr>
<tr><td>Step IV</td><td>Annual Value Amount, ARV = Step I - Step II (if applicable) + Step III</td></tr>
</table></td><td></td></tr>
</table>

S. No.	Minimum Functional Requirements		Compliant (Yes / No)
		Step V: Holding Tax = (13% for holdings in ward nos. 1,2,3,6,31 & 15% for holdings in all other wards) of ARV payable per annum	
		(B) Commercial Holdings (Only hotels, nursing homes, cinema halls, industry, godown)	
		Step I: Plinth Area of the holding in Sq. Meter * No. of Units (A pucca building is normally divided into 9 units i.e. @ 3 units each for floor, wall & roof) * Rs. 478.22 = say X	
		Step II: Take 7.5% of X as erection cost	
		Step III: Depreciate the value obtained in Step II @ 0.5% and taking age of building after 5 years of construction as time	
		Step IV: Take 5% of the land cost where the holding is located	
		Step V: Annual Rental Value, ARV = Step III + Step IV	
		Step VI: Holding Tax = (13% for holdings in ward nos. 1,2,3,6,31 & 15% for holdings in all other wards) of ARV payable per annum	
		(C) Commercial Holdings (other than hotels, nursing homes, cinema halls, industry, godown)	
		Step I: Plinth Area of the holding in Sq. Meter * Rs. 14.30 = say X	
		Step II: Deduct 15% of X towards maintenance cost	
		Step III: Add 5% of the land cost where the holding is located	
		Step IV: Annual Rental Value, ARV = Step I - Step II + Step III	
		Step V: Holding Tax = (13% for holdings in ward nos. 1,2,3,6,31 & 15% for holdings in all other wards) of ARV payable per annum	
		(D) Rented Holdings	
		Step I: Monthly rent of the building * 12 = say X	
		Step II: Deduct 15% of X towards maintenance cost if the holding is more than 5 years old	
		Step III: Annual Rental Value, ARV = Step I - Step II (if applicable)	
		Step IV: Holding Tax = (13% for holdings in ward nos. 1,2,3,6,31 & 15% for holdings in all other wards) of ARV payable per annum	
Integration with GIS			
EGOV/FR/18.24	Visualization of Property details in web based application for citizen		
EGOV/FR/18.25	In case of updating GIS database, department user using needful application and workflow can update the holding/property data.		
EGOV/FR/18.26	Thematic map view for department user to assess holding tax and due for the period.		
EGOV/FR/18.27	User can print WYSIWYG (What You See What You Get)		
EGOV/FR/18.28	The system should have provision using which the citizen can her/his calculate property tax based on attributes, geographical area and other variables using the GIS enablement data of his/her property online.		

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
19. Road Cutting Permission and Restoration		
EGOV/FR/19.1	Application can be registered from any of CFCs/Web Portal/Mobile App	
EGOV/FR/19.2	Workflow based approval for the application by Citizen/Agency	
EGOV/FR/19.3	Online payment facility for Citizen/Agency	
EGOV/FR/19.4	Work list and Dashboard	
EGOV/FR/19.5	Generation of various statistical reports	
EGOV/FR/19.6	Enrolment of ULB officials, Agencies	
EGOV/FR/19.7	Online submission of work request applications by citizens and agencies.	
EGOV/FR/19.8	Captcha text and security question/One-time password feature for security.	
EGOV/FR/19.9	Facility for recording payments made by the applicant in any mode like bank cheque/Demand Draft/Challan.	
EGOV/FR/19.10	Generation of Confirmation receipt.	
EGOV/FR/19.11	Verification of the application at various stages	
EGOV/FR/19.12	Facility for uploading the estimate letter and proceedings by ULB official once the application has been approved	
EGOV/FR/19.13	Facility to check the status of the submitted work request at any stage	
EGOV/FR/19.14	Citizen can raise grievance under a special category in the grievance redressal system.	
EGOV/FR/19.15	Application screening facility to verify the details submitted by the applicant and assign for field verification.	
EGOV/FR/19.16	The Application Verifying Authority should have access to the webpage with authorised User ID and password.	
EGOV/FR/19.17	In case of incomplete application form, the officer in charge can return the same to the citizen for required changes. Citizen shall receive an OTP over e-mail and sms to access the edit feature. On furnishing the same the citizen shall be able to edit the application based on the comments of the verifying officer/authority.	
EGOV/FR/19.18	In case of approved application digitally signed permission letter is generated and shall be available for 30 calendar days.	
EGOV/FR/19.19	Citizen can download the same on successful payment.	
EGOV/FR/19.20	Submission of Completion Report along with date of completion and picture of the site.	
EGOV/FR/19.21	If guarantee is involved, payment refund process is initiated for successful completion report.	
20. Booking of Parks, Community Halls and Other Municipal Properties (water tankers, cesspool vehicles etc.)		
Master		
EGOV/FR/20.1	The system should be able to define master for various municipal properties. - Name/Type of the property - Features available - Capacity - Location - Fees for booking	
Citizen Registration		
EGOV/FR/20.2	The system should allow the users (general citizen, public body and private body) to register themselves by entering the following details:- - Name, age, sex, Aadhaar card no, contact details, etc. - Drop down for Mandap that needs to be booked - Booking amount for the same	
EGOV/FR/20.3	The system should be able to send notification via SMS or email after the successful registration has been done.	
EGOV/FR/20.4	The notification shall contain confirmation of registration, user id and password.	
EGOV/FR/20.5	Now the respective user can log in to the system and the system should allow the user to View and edit their profile.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/20.6	System should allow checking availability for the mandap. The status should show as per the following:- - Booked - Available - Under maintenance	
Booking		
EGOV/FR/20.7	The system should allow the user to book the municipal property	
EGOV/FR/20.8	System should also allow the user to reschedule/cancel the booking	
EGOV/FR/20.9	It should have provision for making the online payment of the booking	
EGOV/FR/20.10	The request for booking shall be sent to the respective official of the department for taking action.	
EGOV/FR/20.11	The official can either approve or reject the booking request.	
EGOV/FR/20.12	The system should also allow the official to escalate the application to the higher authority.	
EGOV/FR/20.13	The notification shall be sent to the respective user about the approval or rejection of booking through SMS or email.	
EGOV/FR/20.14	The intimation shall be sent to the respective user on the confirmation of the booking and payment made.	
EGOV/FR/20.15	The intimation can be downloaded from the system in pdf format.	
MIS Report		
EGOV/FR/20.16	The system shall be able to generate various reports such as - List of booking of various municipal properties (month wise, date wise, etc.) - List of citizens who have booked municipal properties - List of citizen who had booked but cancelled - List of rejected bookings - List of items under maintenance, etc.	
21. No Dues Certificate		
EGOV/FR/21.1	Provision for online application submission with upload of requisite documents for Issue of No Dues Certificate to RMC/RDA	
EGOV/FR/21.2	Provision for tracking status of application	
EGOV/FR/21.3	Facility to online download the certificate	
EGOV/FR/21.4	SMS and Mail alerts	
EGOV/FR/21.5	Integration with required tax modules (Property Tax, etc.) for cross-checking of dues by authorities for issue of No Dues Certificate.	
22. Grievance / Complaint Redressal		
EGOV/FR/22.1	RMC provides various public utility services due to which, it might receive number of complaints/suggestions pertaining to its services. To address all these complaints it is necessary to have an efficient and effective grievance redressal mechanism. It helps in making the administration more accountable, responsive and user friendly. The objective of public grievance monitoring system is to provide multiple channels of grievance recording, in order to make it more citizens friendly and to provide linkages to different sections for increased transparency, citizen participation and performance accountability.	
EGOV/FR/22.2	RMC is very committed to high service levels to its citizens and has multiple mechanisms for citizens to register complaints. Some of these are: Toll-Free helpline number, e-Abhijog (run by the CM's office), a Monday grievance durbar as well as the grievance redressal system developed under the e-municipality project.	
EGOV/FR/22.3	The purpose of this module will be to integrate inputs / complaints received on any of the systems and trigger events in the system for the complaint to be resolved efficiently. The work flows outlined in this document aims at effective monitoring of service levels and reducing repeat complaints.	
EGOV/FR/22.4	Grievance Management system should be a web based application where the citizen can send their concerned grievance & suggestion to the respective departments. The citizen may interact with RSCL and RMC using the portal, the	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	mobile app, the kiosk or approach the citizen facilitation centre. In all these cases the work flow shall proceed from the portal.	
EGOV/FR/22.5	Once the grievance is received, it should have a work flow to trigger an event in the system. The module should have a comprehensive Service Delivery Framework which – - Is easily accessible - Responsive to citizen's needs - Enables quick decision capability - Connects all stakeholders with right kind of information in the quickest possible timeline - Allows all stakeholders clear visibility and communication	
EGOV/FR/22.6	The solution should offers citizens ability of reaching out to RMC through variety of options to ensure broad based participatory framework of communication, thus enabling wider participation from citizens to improve service quality and civic liveability quality. The proposed system shall offer multiple options by way call-centre desk, walk-in at respective ULB offices, online through web portal, SMS & E-Mail, Web App, Mobile App, IVR, Call back service etc., to register a complaint. Further, a time bound call centre is also being proposed to support and manage in and out calls to and from Citizens. All complaints are to be allocated, routed and managed through an automated algorithm which is designed to identify actual resource within RMC to manage the complaint and thus removing human interface to work assignment. Further, concerned higher authorities within RMC are to be empowered with real-time mobile Apps and web Apps to monitor the complaint resolution process and capability to intervene if necessary, to help them in decision making process to take needful corrective actions. The system should automate enforcement of SLA policies and streamline and automate every process from initial citizen request to resolution more efficiently and cost effectively.	
EGOV/FR/22.7	The system should be capable of communicating with citizens and officers alike about the status and tracking of the complaints via SMS and email including unique tracking numbers.	
EGOV/FR/22.8	The complaint redressal system should enables configuration of RMC's respective geographical and administrative jurisdictions including service delivery essential information. The highest office in government pertaining to RMC management should have access capability to aggregated data and analytics from all the wards within the system.	
EGOV/FR/22.9	The system should have the ability to maintain different types of grievances caused to the citizens, department or section that needs to address the grievance, number of days within which the grievance needs to be addressed and nature of grievance whether it is financial or non-financial.	
EGOV/FR/22.10	It should have the ability to maintain the statuses of the grievances registered in the municipality. Also the ability to maintain the details of work/application that has not been addressed within the prescribed time, number of days of delay and compensation paid per day in case of delay in SLA of the grievances registered in RMC.	
EGOV/FR/22.11	The system must maintain the details of officers designated to redress grievances mapped to the department-section and the compensation details from the officer responsible and payment details to the citizens if the applications are not processed within the prescribed time. (Breach of SLA).	
EGOV/FR/22.12	On sending the grievance & suggestion the department officials are bound to respond to the grievance & suggestion as per the specified time frame. All grievances & suggestion would be allotted a unique number which would be the base for further correspondence. There would be automatic escalation plus provision for RMC staff to post confirmation of a 'before' and 'after' of the complaint. Following reports shall be generated by the applications: - All grievances registered during a given period - Pending grievance registered during a given period - Disposed grievance during a given period	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Duration of grievances registered during the period - Repeated grievances registered during the period	
EGOV/FR/22.13	All these reports can be generated departmental wise, grievance wise, department & grievance wise. On the basis of these reports analysis can be made and decisions shall be taken by government officials.	
EGOV/FR/22.14	Modes of complaint registration - Through phone at call centre - Walk-in to a ULB office location - Online through web portal - Through E-Mail - Through SMS - Mobile App - Through IVR - Based on Recorded details - Call Back - Other existing complaint systems	
EGOV/FR/22.15	The system should be capable of converging information management and delivery system, which enables calls, collected through different communication channels to be converged on to the common distribution system and hence brings in commonality in allocation and response mechanism.	
Complaint Registration		
EGOV/FR/22.16	Through Call Centre (Phone, e-Mail & SMS) - A citizens calls designated telephone number - Call centre operator registers the single or multiple complaints with required details - Complaints through e-Mail / SMS shall be received at call centre - Complainant shall be communicated the complaint tracking number(s) generated by the system and acknowledgement SMS send to the registered mobile number.	
EGOV/FR/22.17	At ULB Location - Citizen visits the ULB location in person to get his / her complaint registered - Complaint shall be registered in the system with all due details and a printed acknowledgement receipt shall be given to the citizen.	
EGOV/FR/22.18	Through Website - Citizen shall be able to register his / her complaint on website and can print acknowledgement receipt	
EGOV/FR/22.19	Through IVR - Citizen calls on the designated number - This feature shall be available when Call centre is not operational i.e. during non-working hours or when all lines at the call Centre are busy. - In case all the activated extension numbers are engaged with other calls or operator not available to receive calls, the IVR system activates call waiting message for the caller with the option to either wait or option to dial 9 and give missed call for call back to caller or register call via voice recording. - IVR system shall record the complaint details provided by - IVR system shall record the complaint details provided by the citizen during the call - Call centre operator registers the complaint based on the details provided in recording or calls back the citizen to register the complaint - Citizen is given a complaint registration number via SMS	
Complaint Allocation		

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/22.20	Once a complaint is registered with the system, it automatically is assigned to a concerned area officer dealing with the problem based on the scientific algorithm engine built in to the system and allocation matrix defined. The system should automatically send an SMS to officer alerting him / her on the complaint. Application should offers following definable Allocation methods - Workload based allocation - Round robin allocation based on SLA hours - Sequential allocation of complaint to each member of the team If the complaint is not resolved and closed within the specified period, the same should get escalated to higher authorities. The allocation and escalation process should be fully automated and not require any human intervention; however, system should provide a feature to switch to manual allocation, if needed	
Field Call Report in case of citizen area visit		
EGOV/FR/22.21	The RMC officer updates the details of the work done along with the status of the complaint (Pending / closed) in the system against each FCR. The system shall maintain the history of the work done.	
Complaint Closure		
EGOV/FR/22.22	The officer needs to resolve a complaint within a specified SLA period. Once a complaint is resolved, the officer fills a field call report and submits to a superior, who in turn calls the complainant to seek his / her satisfaction on the measures undertaken to solve the problem. If the complaint is not redressed within a fixed number of hours, the system shoots off SMS to higher officials in hierarchy based on the escalation matrix defined.	
Complaint Re-open Process		
EGOV/FR/22.23	The Citizen has option to re-open his / her complaint if not satisfied with the services rendered. The Citizen can request to re-open the complaint via Email or Phone or SMS. Any complaint can be re-opened only if it is within the SLA or re-open hours set for that complaint. All re-opened complaints shall be escalated to concerned senior officials.	
Complaint Status		
EGOV/FR/22.24	The Citizen should be able to know the status of his / her complaint online from website or through phone / SMS.	
Citizen Feedback		
EGOV/FR/22.25	Citizen should have an option on the website to voluntarily provide their feedback on the complaint redressal process and also to comment on the satisfaction/dissatisfaction received by them while using the system.	
Problem Category & SLA		
EGOV/FR/22.26	The various problems, for which the complaints are raised, could be part of a particular Department. These problems are categorized as Drainage Maintenance, Footpath, Roads etc. could be part of Engineering department & Traffic signal/Central Verge plantation site, Tree cutting/trimming related problems could be part of Garden department. Application Administrator should be able to define standard SLA hours, problem category and problems. The application administrator shall be - Able to add/edit/delete standard SLA. - Able to add/edit/delete different type of problem category. - Able to add/edit/delete problems under problem category. - Able to attach standard SLA hours and department to each problem. - Admin shall be able to change status of problem category in active/inactive state.	
Holiday, Department, Designation, Employee		
EGOV/FR/22.27	The application administrator should be able to manage RMC's holiday calendar,	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	department, designation and employee details in the system.	
Allocation & Escalation Matrix		
EGOV/FR/22.28	The application administrator should be able to maintain allocation matrix for the RMC's employees in resolving the various categories of problems for the area for which he / she is responsible to look at. This setup helps the Automatic Complaint allocation to the employees. Set the priority based on which the selected employee will receive the complaints for the selected department's problem category of his/her area. The application administrator should be able to set up the escalation matrix for each department at the various levels and to define what should be the mode of escalation communication for each of these levels and define their frequency. The system automatically escalates the complaints based on SLA, escalation matrix and the frequency defined.	
Area Mapping, Area Transfer, Employee Transfer		
EGOV/FR/22.29	Complaint allocation process should be tightly integrated with RMC's area, employees and complaints. Based on the problem location, the complaint should get allocated to the RMC official. Each area of a city is mapped with the RMC's operational area and each employee is mapped with location & department. The application administrator can transfer area from one operational area to another as well as an employee from one location to another. The transfer process shall be designed in such a way that all pending complaints shall be automatically be detached from the employee being transferred and the same shall be either automatically attached to the peer or higher official in hierarchy.	
Complaint Transfer		
EGOV/FR/22.30	ULB Official can transfer his / her pending complaints to another official from the same or different area / location.	
Management Information System		
EGOV/FR/22.31	Exhaustive reports ULB be generated by the system for officers at various levels for effective decision making and period review of operations. Some of the MIS reports generated from the system will be as follows: - Department Wise RMC Location wise SLA Summary (Within SLA v/s Beyond SLA) - Registration Mode wise Complaint Summary - Department wise ULB Location wise Average TAT Report - RMC Location wise TAT - Detailed Complaint Report with FCR - Detailed Complaint Report without FCR - SLA Wise Ageing Details - Location wise Complaint Status Summary - Complaint Transfer Summary - Department wise weekly status report – Registered, Closed, Within SLA / Beyond SLA - Reopen Complaint As on Date with complaint status - Location wise Registered v/s Closed Complaints - Missed call Detail - RMC Employee Reporting Hierarchy - List of on hold complaints - Operator wise / Location wise Login-Logout Report - List of mobile numbers from which complaints registered - List of complaints Transferred - RMC Location wise Standard SLA v/s Actual TAT report	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	Real-time statistical reports for RMC locations/departments is made available to senior officers on web based as well as on based mobile applications.	
Dashboard		
EGOV/FR/22.32	Real-time processed information immensely aid senior officials in taking immediate corrective and preventive measures. Analytical reports help administration in identification of areas of concern and root-causes. The Grievances System shall provide a real-time dashboard.	
Service Analytics Engine		
EGOV/FR/22.33	The system should provide DIY (Do it yourself) data analytics platform based on the philosophy of analytics for all. The platform should provide a simple query bar and users can input their analytics requirements using a DRAG and DROP functionality. This offers enormous ease and ability to any kind of user irrespective of IT knowledge to mine high level analytics reports from the service data. The system should consume structured, semi structured and un-structure data to offer capabilities like deep web analytics. The system should offer advanced abilities such as: - Prescriptive analytics - Predictive analytics - Diagnostic analytics This ensures that users at different level can mine intelligence at click of a button which would aid policy decisions and empower the users to take quick and informed decisions.	
23. Web Based GIS		
EGOV/FR/23.1	The proposed Geospatial layer for different municipal functions will be as follows: - Municipal Boundary - Plot details - Property data - Land use: Residential, mixed, commercial, group housing, industrial, institutional, recreation, green areas/parks - Roads - Street lights - Water Supply lines: Supply lines, overhead tanks, valves, boosters - Storm water drains: Drainage networks, inlets - Sewage Lines: Sewage network and main holes - Electricity lines: electricity poles, substations, High tension lines. - Monuments and Heritage sites - Solid waste disposal sites, Septage Treatment Plant and location of community bins/ garbage depots, septic tanks/containment units - Education Institutes - Health centres - Advertisement hoardings - Markets - Police stations/ chowkis - Post offices - Banks - Fire stations	
EGOV/FR/23.2	GIS integration aims at editing and publishing all the assets under RMC for better information management, accurate estimation and tracking. These assets can be streets assets, building assets, public assets and other transport and utility network.	
EGOV/FR/23.3	All the GIS layers are to be built for RMC and the MSI is expected to create a web service according to the following requirements and publish it, along with customization of the application to integrate with e-governance modules and query	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	modules. The MSI has to update the GIS data in the TSCL period.	
EGOV/FR/23.4	RMC wishes to have 2 main views for publishing. - Public view: for common people who may view the vacant and occupied plots with all its attributes: dimensions, distance from roads and neighbouring plots, current land use and market value. - Second related view will be for Industrial or Citizen Residents. The query can be initiated using the resident id for access. In this view, ownership and tax details can be visible. - The detailed view will be for internal or city manager users. Here depending on authorisation level, data may be displayed. The editing rights of spatial and non-spatial data are with the city manager.	
EGOV/FR/23.5	The MSI shall keep the assets and their attribute information up-to-date. - Street Assets: Benches, street lights, traffic signals, signposts, garbage cans, fire hydrants, bus stops, bridges, overpasses and underpasses, tunnels, culverts, and guardrails. - Pipeline Network: Water supply system - Drainage Network: Rivers. - Utility Network: Electricity, cable, telephone. - Transport Network: Roadways, Rivers - Fleet Assets: Garbage trucks, ambulances, police vehicles, fire tenders, transport vehicles, construction equipment, and other vehicles. - Building Assets: Government offices, public buildings, educational buildings, public safety buildings, historic buildings, and sporting facilities. - Other Public Assets: Tourist facilities, religious facilities, monitoring stations, water and sewerage treatment plants, water wells, springs, reservoirs, dams, parks and playground equipment, trees, and car parks	
EGOV/FR/23.6	RMC internal users will require the following integration with the e-governance application: - Property Tax - Asset management- water, drain, sewage, electricity - Grievance redressal - Waste management - Utility payments - Land management system	
EGOV/FR/23.7	The integration has to be done on the concerned layer. The following are few of the integration points with the e-governance module	
Property tax		
EGOV/FR/23.8	The attribute data with the property must store (but not limited to) data such as: - Property location geographic - Property location address - Status (vacant / sold) - Current use - Owner ship details - Property tax details - Utility details	
EGOV/FR/23.9	The user could: - Searching of Property Index Number - Property Tax link should be integrated and will have option to direct: - Property Tax-> Search on online receipt - Property Tax-> Search Ledger - Property Tax-> Pay online	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- GIS Application to Property Tax Module - Property Owner can be selected on the basis of : - Administrative boundary - Property Index Number - Property tax range selection - Period Selection - Who has paid, not paid. - On the basis of above search criteria, the selected Property data should be extracted: - Details of Property owner like Name, Address, PIN. - Details of Arrears There should be a link in Property Tax module for GIS View to drive into GIS Application to View/Analyse the property geographical locational details i.e. address, Plot Area, constructed area, etc.	
The Utility Asset Management Module:		
EGOV/FR/23.10	The GIS has to integrate with asset data of roads, water supply lines, sewage lines, storm water drains, electricity lines. The attribute shall include the following: - The location details - The geometry details - The engineering details - The attached property details	
EGOV/FR/23.11	The sub-modules should have the following functions: - GIS based Asset data visualization - GIS based asset maintenance management - GIS based asset construction management - GIS based web ticketing for complaint registration and solution	
EGOV/FR/23.12	The user should be able to annote the Place where the asset management activity is proposed by inserting a point/Line on the map and shall be created and saved in Project layer. A query can be generated on the project layer for Project Name, Functional Group, Budget, Project date and Project status. This may be accessed by other departments which will be affected by the project work.	
GIS Application integration to Asset Management		
EGOV/FR/23.13	Searching of Zone/Ward/ GIS layers:	
EGOV/FR/23.14	Built-up area for any property maintenance and Rent	
EGOV/FR/23.15	Land use land cover (LULC) area for Vacant land	
EGOV/FR/23.16	Transportation for any road maintenance	
EGOV/FR/23.17	Sewage and Drainage for Maintenance	
EGOV/FR/23.18	Public Lighting for maintenance	
EGOV/FR/23.19	The Vacant Land will be linked with Asset Management-Asset Report-Asset Category-Market Value	
EGOV/FR/23.20	This will be integrated with rent & maintenance	
EGOV/FR/23.21	Query can be generated on project layer for Rent: Rent Type, Rental amount, Renewal date & Land: Market Value	
EGOV/FR/23.22	The Building properties will be integrated with- Asset Management	
EGOV/FR/23.23	Property Index Number	
Waste management module		
EGOV/FR/23.24	Property Index Number indexed with Garbage Collection Point (GCP), septic tanks/containment units	
EGOV/FR/23.25	Category of garbage collection points, septic tanks/containment units will be queried and viewed on Map based on PIN	
EGOV/FR/23.26	Waste Management-Reports-PIN, Category.	
24. KPI's and Dashboard		

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/24.1	Performance management, monitoring and evaluation are critical elements utilized by the city to improve organisational and individual performance and to enhance service delivery. The establishment and development of the performance management framework ensures integration between strategic planning and performance management by linking the solutions/services to indicators and targets that can be used to measure performance. Following is the proposed performance management framework, which is developed based on global city performance framework like ISO: 37120 and others	
EGOV/FR/24.2	Service Performance: Measures the performance of citizen services across areas like energy, waste, mobility, etc. to ensure more effective governance and delivery of services. Following are some of the illustrative performance indicators to assess performance across the areas of service performance: - Total electricity energy use per capita - Response time for emergency response services from initial call - Response time for fire department from initial call - Total number of registered users in the portal and users registered in a particular month/year. - Percentage of citizens using online services - Average delay in grievance redressal - Tax collected as percentage of tax billed - Percentage of school-aged population enrolled in schools (Male/Female) - Percentage of schools with access to digital education - Number of in-patient hospital beds per 10,000 population - Number of fire fighters per 100,000 population - Number of police officers per 100,000 population - Percentage of city population living in slums - Number of homeless per 100,000 population - Percentage of city population with regular solid waste collection - Percentage of city population with potable water supply service - Household level coverage of direct water supply connections - Per capita supply of water - Quality of water supplied - Level of non-revenue water – NRW - Percentage of water connections covered through meters - Number of internet connections per 100,000 population - Number of personal automobiles per capita - Percentage of people using public transport to work - Doctor patient ratio in city hospital - Geographical coverage of public transport - Availability of public transport - Percentage of road network with dedicated bicycle tracks - Percentage of interchanges with bicycle parking facilities - Mode share of non-motorised transport - Availability of Passenger Information System - Percentage of city population with authorized electrical service - Percentage of electrical connections covered through smart meters - Average number of electrical interruptions per customer per year - Average length of electrical interruptions per customer per year - Extent of signal synchronisation - Availability of paid parking spaces - Percentage coverage of footpaths – wider than 1.2m	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Percentage of traffic intersections with pedestrian crossing facilities - Extent to which universal accessibility is incorporated in public rights-of-way - Household level coverage of municipal solid waste collection	
EGOV/FR/24.3	Social Performance: Performance management solution to monitor and track the performance of social services like health, education, safety, etc. This will help the municipals to assess whether the current state of these services is optimum and/or what are the improvement opportunities. Following are some of the illustrative performance indicators to measure social performance: - Percentage of students completing primary/secondary education - Primary education student/teacher ratio - Number of higher education degrees per 100,000 population - Number of physicians per 100,000 population - Percentage of convictions and case closure for criminal cases - Number of recorded crimes per lakh population - Extent of crimes recorded against women, children and elderly per year - Transport-related fatality per lakh population - Citizen score for city governance - Citizen score for citizen services - Doctor patient ratio in city hospitals - Number of streets, public places, junctions covered through surveillance systems - Coverage of toilets - Collection efficiency of sewerage network - Coverage of sewerage network and/or septage - Extent of reuse and recycling of waste water - Coverage of storm water drains - Efficiency of collection of municipal solid waste - Extent of municipal solid waste recovered through reuse - Quality of water in public surface water bodies	
EGOV/FR/24.4	Environmental Performance: Measurement of environmental health of the city to assess how good or bad is the state of environment and the areas the city needs to focus on for improvements. Following are some of the illustrative performance indicators to measure environmental performance: - Particulate matter concentration - Greenhouse gas emissions measured in tones per capita - NO2 concentration - SO2 concentration - O3 concentration - PM10 concentration - Noise pollution - Green area (in hectares) per 100,000 population - Annual number of trees planted per 100,000 population - Per capita availability of green spaces - Per capita availability of public and recreational places - Percentage of new and redeveloped buildings following green building norms - Percentage of plots with rainwater harvesting facility - And many more	
EGOV/FR/24.5	Economic Performance: Measurement of the state of the city's financials to track and monitor aspects like city's revenue generation, budgets, expenditure, industrial expansion, businesses development, employment, poverty etc. with the aim of making a city self-sustaining and increasing its revenue generation. Following are	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	some of the illustrative performance indicators to measure economic performance: - City's unemployment rate - Assess value of commercial and industrial properties as a percentage of total assessed values of all properties - Percentage of total energy derived from renewable sources - Energy consumption per unit – water supply and sewerage - Energy consumption per unit – street lighting - Total energy consumption per capita - Percentage of city population living in poverty - Percentage of people in full time employment - Youth unemployment rate - Number of businesses per 100,000 population - Capital spending as a percentage of total expenditures - Own-source revenue as a percentage of total revenues - Tax collected as a percentage of tax billed - Increase in VAT /GST collection - Increase in collection of Professional Tax - Increase in issuance of Construction Permits - Percentage of vendors registered and provided formal spaces - Percentage of Slum/EWS households covered through formal/affordable housing - Percentage of slum areas covered through basic services	
EGOV/FR/24.6	The exact parameters will be finalized during implementation. However a performance management dashboard has to be provisioned and a facility to collect the information requirement for Dashboard has to be provisioned through Portal solution. It may also require integration with various information providers. MSI will be responsible for complete solution design along with integration with information sources for respective indicators. Wherever information needs to be collected from stakeholders residing in the township or entrepreneurs or various facilities in the township, portal solution will need to be developed by MSI so as stakeholders can provide the information required and the same can be presented on KPIs and dashboard.	
25. Revenue from Property Taxes, Land Leases & Other services		
EGOV/FR/25.1	Detailed property tax functionality is given in the sections under e-governance. Functionality given below with respect to property tax is additional.	
EGOV/FR/25.2	Property Tax: Creation of a sales order for property tax for each leased plot as well as periodic billing with functionality for : - The user to modify the property tax rates with history being maintained of the old rates - Property tax rates may vary from plot to plot and/ or customer to customer - Billing frequency of property tax may vary from plot to plot and/ or customer to customer - System should allow payment of early payment discounts - System should provide functionality for auto-generated reminder letter for unpaid property tax bills with automatic calculation and levy over interest and/or penalty Tracking of payments received against property tax bills	
EGOV/FR/25.3	Interfacing (real time) shall be required with the Land Management System.	
EGOV/FR/25.4	Submission of property tax in subsequent years with changes or without changes in property details like structure, usage etc.: - Capture details of multiple owners - Handle listing of multiple usage types within a property - Handing rebates, specific standardized rules, and considering various factors while calculating ARV of the property.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	Capturing floor wise details in case of buildings	
EGOV/FR/25.5	Functionality of Self-Assessment, subsequent assessments filed by the Citizen and making changes if any by RMC or RSCL.	
EGOV/FR/25.6	Functionality for revising property tax rates about issuing a notice to the owner/occupant informing him/her about the revision of rates. In case of joint ownership, functionality should provide for issuing notices to multiple parties. The address of these parties may not be the same as the property address and the system must be capable of storing these multiple address as per business requirement.	
EGOV/FR/25.7	Functionality for occupants/owners to file an objection against the revision notice.	
EGOV/FR/25.8	Fixing a Hearing in response to an objection by a citizen and issuing and intimation electronically and/or in letter format. The system should also provide the functionality to capture the proceedings of the Hearing and generating a final Hearing Order.	
EGOV/FR/25.9	Yearly property tax bill generation – handling arrears, penalty/interest, advance and self-assessment payments. There may be more than one component in the property tax bill like service tax or GST. The amounts against these components should be indicated clearly as separate line items	
EGOV/FR/25.10	Collection of tax payments with automatic bifurcation in predefined proportion or as per priority defined with handling of rebates for early payments	
EGOV/FR/25.11	Functionality for mutation (change in ownership) of property through heredity or by sale of property.	
EGOV/FR/25.12	Functionality for occupants/owners to file an objection against the mutation.	
EGOV/FR/25.13	Fixing a Hearing in response to the mutation objection by a citizen and issuing and intimation electronically and/or in letter format. The system should also provide the functionality to capture the proceedings of the Hearing and generating a final Hearing Order.	
EGOV/FR/25.14	Revaluation of Property upon survey/ identification of change in property by RMC.	
EGOV/FR/25.15	Customer Facilitation Centre: - Issue of transfer certificate - Issue of property tax assessment certificate - Issue of property extract Issue of duplicate bill	
EGOV/FR/25.16	Functionality to upload existing property records with outstanding as on cut-off date that is available in digital format. System must provide functionality for manual data entry through user friendly online screens of such data	
EGOV/FR/25.17	Day to Day property tax related reports as per business requirement including interactive reports catering to what if scenarios	
EGOV/FR/25.18	Integration of property tax billing and collection status with GIS for visual display	
EGOV/FR/25.19	Advertisement Hoardings: - Creation of a sales contract and subsequent billing from advertisement hoardings - Registration of media agencies as customers - Functionality for booking an advertisement - Functionality for setting up new hoarding and display of advertisement Functionality for renewal of advertisement contract	
EGOV/FR/25.20	RMC users must be able to carry out processes on the system like Contract Entry, Billing, Collection, Issue Renewal Notices, Contract Renewal, Suspension and Cancellation	
EGOV/FR/25.21	Rechargeable Work: creation of a sales order and raising an invoice for work done which is chargeable to a customer	
EGOV/FR/25.22	Usage of Telecom Fibre Network : creation of a sales order and raising an invoice for usage of fibre by telecom services providers: - Fixed rental basis Percentage of revenue basis	
EGOV/FR/25.23	Parking Lots: Creation of a sales order and subsequent billing from parking lots	
EGOV/FR/25.24	Miscellaneous Revenues: Functionality to account for miscellaneous revenues from digital services, or rental for usage of community halls etc.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/25.25	Reports as per business requirements of RMC relating to Revenue from Property Taxes, Land Sales, Telecom Fibre Usage etc.	
EGOV/FR/25.26	Rent and Lease: - Booking of Estate - Rent Payment schedule - Department process like Contract Entry, Billing, Collection, Renewal Notice, Contract Renewal. Reports	
EGOV/FR/25.27	Advertisement & Hoarding (contract management): - Registration of Media Agency - Application for booking of advertisement - Setting up new hording and display of advertisement - Renewal of Advertisement contract - Department process like Contract Entry, Billing, Collection, Renewal Notice, Contract Renewal, Suspension, Cancellation	
26. Finance and Management Accounting		
General Ledger		
EGOV/FR/26.1	Multi-currency functionality support and Indian GAAP (generally Accepted Accounting Principles) compliant ledger	
EGOV/FR/26.2	Functionality to define chart of accounts at group and entity level	
EGOV/FR/26.3	A robust journal with complete traceability of financial transactions. Entry deletion must not be allowed. Automatic reversal functionality must be provided for reversing transactions	
EGOV/FR/26.4	Posting of Transactions and Opening & Closing Periods	
EGOV/FR/26.5	Facility to create draft transactions with auditable transaction numbering feature	
EGOV/FR/26.6	Automatic transaction posting feature	
EGOV/FR/26.7	Feature to open and close financial periods	
EGOV/FR/26.8	Feature for adjustment periods in addition to the normal 12 periods for posting transactions in any financial year	
EGOV/FR/26.9	Feature to allow soft close and hard close of financial periods	
EGOV/FR/26.10	Restrict transaction posting only to open periods	
EGOV/FR/26.11	Capability to drill down into transaction details from period balances	
EGOV/FR/26.12	System should have functionality to maintain plan financial statements for any business unit within a legal entity or at corporate group level	
EGOV/FR/26.13	Facility to have hierarchical account structure	
EGOV/FR/26.14	System should allow maintenance of multiple plans for any financial year	
EGOV/FR/26.15	Provide the flexibility to record financial transactions for multiple legal business entities and generate required statutory financial statements like Profit & Loss, Trial Balance, Balance sheet and reconciliation reports for each entity	
EGOV/FR/26.16	Provide functionality for automated consolidation of accounts with out of the box functionality for setting-off of inter business entity payables and receivables consolidation of investments and multi-currency valuation	
EGOV/FR/26.17	Automatic generation of trial balance	
EGOV/FR/26.18	Provide functionality for the user to define the format and contents of financial statements.	
EGOV/FR/26.19	Provide multiple reports as required by users for monitoring and control purposes.	
EGOV/FR/26.20	Payments and Bank Reconciliation - Cash management forecast functionality Bank transactions including reconciliation	
EGOV/FR/26.21	Manage incoming electronic payment and transfer of funds including net banking, credit cards or any other payment mechanism. Applicable for domestic(INR) and overseas payments in foreign currency	
EGOV/FR/26.22	Manage outgoing electronic payment and transfer of funds including net banking, credit cards or any other payment mechanism. Applicable for domestic in INR and overseas payments in foreign currency	
EGOV/FR/26.23	Process cash and cheque payments with automatic handling of outstation cheques in Indian of foreign currency	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.24	Re-grouping of GL balances according to pre-defined rules for statutory reporting; system should provide necessary information for preparing year end schedules for audit purposes	
EGOV/FR/26.25	Re-valuation of balances and open transactions in foreign currency according to local and global accounting standards	
EGOV/FR/26.26	The system should be able to generate a payment acknowledgement as and when required.	
EGOV/FR/26.27	System should have functionality to manage travel management and other transactions related to employees; should have functionality to maintain account for each employee	
EGOV/FR/26.28	Manual and automated cheque printing.	
EGOV/FR/26.29	Facility for preparing a forecast with varying time horizons. Provision required for automatic bank reconciliation	
EGOV/FR/26.30	Taxation, duties and levies accounting of tax transactions, detailed information flow, challan preparation and filing of different tax returns according to federal as well as state government legal requirements.	
EGOV/FR/26.31	Facility to maintain accounts as per Indian statutory requirements.	
EGOV/FR/26.32	Compliant with the GST procedures to be implemented in India. Facility to have multiple tax structures on transactions	
Accounts Payable		
EGOV/FR/26.33	Multi-currency functionality	
EGOV/FR/26.34	Automatic reconciliation of sub-ledgers with the control account in the General Ledger	
EGOV/FR/26.35	User must be able to create/maintain Vendor master record. Common master data of vendors with procurement is required	
EGOV/FR/26.36	Functionality to process one off payments for vendors with whom RMC does not intend to have a long term business relationship and maintain a separate master data record	
EGOV/FR/26.37	User defined facility to classify vendors in groups and assign separate number ranges. These number ranges could be assigned externally or internally by the business entity. The external number require flexibility to have alphanumeric characters	
EGOV/FR/26.38	System should allow fast data entry of invoices based on purchase order etc.	
EGOV/FR/26.39	The system must allow the business entity to assign vendors to separate control accounts in the general ledger	
EGOV/FR/26.40	System should provide functionality for electronic approvals of invoices based on preconfigured rules	
EGOV/FR/26.41	Functionality to block process vendor payments in case of dispute at invoice level or vendor level	
EGOV/FR/26.42	System must handle multiple modes of payment including electronic and must generate output as required by banks	
EGOV/FR/26.43	System must have necessary controls for managing sensitive information for vendors e.g. vendors' bank accounts	
EGOV/FR/26.44	Recording and monitoring of bank guarantees	
EGOV/FR/26.45	System should provide functionality at master data level of vendors to restrict operations of these accounts only by a certain set of employees	
EGOV/FR/26.46	System must allow monitoring of advances given to vendors	
EGOV/FR/26.47	Functionality for processing of payments for vendors with automatic vendor account posting and clearing	
EGOV/FR/26.48	Automatic system calculated TDS deductions for vendor payments	
EGOV/FR/26.49	Automatic posting of input tax (GST) whilst vendor invoice processing	
EGOV/FR/26.50	Functionality of automatically handling re-imbursement of expenses like transport, insurance during vendor invoice processing	
EGOV/FR/26.51	Whilst processing payments either automatically or manually, for vendors, the system should allow the advances to be adjusted partially or fully	
EGOV/FR/26.52	Facility to issue credit/ debit notes by the system	
EGOV/FR/26.53	Functionality for handling imports with T/T and L/C Process	
EGOV/FR/26.54	Functionality for system generated letters to vendors for balance confirmations	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.55	Out of the box availability of reports for vendor reconciliations and other reports as per user requirement.	
EGOV/FR/26.56	Out of box functionality for online inquiries on vendor balances on various parameters and statuses	
EGOV/FR/26.57	System should have a strong reporting functionality that includes analysis of vendor master data, open invoices, overdue payments, payments made in advance, blocked invoices report etc.	
Accounts Receivable		
EGOV/FR/26.58	Multi-currency functionality is required	
EGOV/FR/26.59	Automatic reconciliation of sub-ledgers with the control account in the General Ledger	
EGOV/FR/26.60	User must be able to create/maintain Customer master record. Common master data of customers with sales/invoicing is a requirement	
EGOV/FR/26.61	Functionality to process invoices of one time customers where RMC does not wish to maintain a master debtors record	
EGOV/FR/26.62	Facility to classify customers in groups and assign number ranges. These number ranges could be assigned externally or internally by the business entity. The external number range may have alphanumeric characters	
EGOV/FR/26.63	The system must allow the business entity to assign separate control accounts for customers in the general ledger	
EGOV/FR/26.64	Functionality to block posting customer accounts	
EGOV/FR/26.65	System should provide functionality at master data level of customers to restrict operations of these accounts only by a certain set of employees	
EGOV/FR/26.66	System must allow monitoring of advances received from customers	
EGOV/FR/26.67	Automatic processing of receipts via cheque, electronic funds transfer or other means with auto posting of output tax which may be in the form of GST, VAT, sales tax, service tax or any other municipal levy. There could be business instances of more than one central tax, state tax or municipal levy	
EGOV/FR/26.68	While processing receipts either automatically or manually, for customers, the system should allow the advances to be adjusted partially or fully. The posting to customer debtors account should be automatic with clearing of the required entries	
EGOV/FR/26.69	Facility to issue debit notes and/or credit notes as applicable with ability to provide discounts and rebates	
EGOV/FR/26.70	Automatic interest calculation for overdue payment. The system must allow the user to specify the interest rates for a customer or a group of customers	
EGOV/FR/26.71	Functionality for automatic generation of reminder letters for overdue payments in the accounts receivable. The letter format should be user definable	
EGOV/FR/26.72	System should have functionality to provide reports including open customer invoice, payments received (partial or full), ageing analysis according to overdue dates	
Asset Financial Management		
EGOV/FR/26.73	Generate automatic asset numbering as well as manual numbering	
EGOV/FR/26.74	Maintain detailed information per asset item: asset description, asset class, asset serial number, asset bar code, location, asset main category and sub category, department/cost centre, custodian, employee number, purchase date, depreciation start date, service start date, vendor, PO reference, invoice reference, warranty start date, warranty end date, acquisition cost, salvage value, useful life and depreciation method and any other relevant asset information	
EGOV/FR/26.75	Maintain collective information of low value assets like items of furniture	
EGOV/FR/26.76	Define parent child asset relationships	
EGOV/FR/26.77	Add additional upgrading cost to an existing asset. System should provide a report showing the history of upgrades and also include the addition into the new depreciation run over the remaining period of the asset. E.g.: Capital construction projects	
EGOV/FR/26.78	Capture work in progress (WIP)/construction in progress (CIP) assets and later on convert them as normal assets and start depreciating	
EGOV/FR/26.79	Add WIP/CIP expenditures to an existing CIP assets through the accounts payable system	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.80	The asset system should be allowed to be marked as physical inventory tracking asset and should generate physical inventory reports	
EGOV/FR/26.81	Ability to split an asset into multiple assets	
EGOV/FR/26.82	System should be able to depreciate assets using common depreciation methods: - Straight line - Double declining balance - Written down value method - User defined method of depreciation Number of hours etc.	
EGOV/FR/26.83	Ability to calculate depreciation based on groups of assets: - By department By cost centre	
EGOV/FR/26.84	Ability to recalculate depreciation on asset: - Based on a change in value - Based on a change in depreciation schedule Based on a change in asset life	
EGOV/FR/26.85	Ability to capitalize assets	
EGOV/FR/26.86	Ability to perform “un-planned" depreciation	
EGOV/FR/26.87	Ability to automatically process and post transactions: Depreciation expenses Cost Adjustments, if any	
EGOV/FR/26.88	System should allow user definable depreciation formulas	
EGOV/FR/26.89	Ability to define depreciation conventions, such as Mid-Month convention, End-of-the-Month Convention etc.	
Asset Transfers		
EGOV/FR/26.90	Transfer assets between: - Divisions/Departments/Cost Centres - Locations - Custodians - Projects - Work Package (within a project) Job (Specific activity within the work package)	
EGOV/FR/26.91	Transfer all or part of an asset	
EGOV/FR/26.92	Transfer groups of assets	
EGOV/FR/26.93	Ability to generate transfer slips in case of asset transfers	
Assets Retirements		
EGOV/FR/26.94	Fully retire	
EGOV/FR/26.95	Partially retire	
EGOV/FR/26.96	Retire by units	
EGOV/FR/26.97	Retire by cost	
EGOV/FR/26.98	Reinstate retired assets	
EGOV/FR/26.99	Ability to process sales of fixed assets with the Automatic creation of gain/loss transactions	
EGOV/FR/26.100	Different retirement accounts for gains and losses	
Revalue assets		
EGOV/FR/26.101	Revalue assets (change the basis of depreciation and net book value) and adjust the cost of an asset, e.g. capitalization of renovation cost, useful life, depreciation % and write off amounts	
EGOV/FR/26.102	Ability to revalue a single asset or group of assets based on percentage or value	
EGOV/FR/26.103	Ability to record and amortize revaluation reserve based on International accounting standards	
Physical verification		
EGOV/FR/26.104	Ability to maintain a physical control of assets and be able to track assets by serial number, asset number, custody number and project/ cost centre/ location.	
EGOV/FR/26.105	Ability to create a Fixed Assets Verification Sheet, containing asset code, location, physical balance.	
Insurance		

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.106	Ability to track asset insurance details such as sum insured, premium etc.	
EGOV/FR/26.107	Ability to generate a report showing insurance expiry dates	
Reports		
EGOV/FR/26.108	Generate fixed assets register by: - Department/Section - Location - Gain and Loss on asset sales - Projected Depreciation - Custodian - Cost Centre wise - Period depreciation reports – summary - Asset depreciation per period Period	
EGOV/FR/26.109	Generate asset depreciation register (detail and summary)	
EGOV/FR/26.110	Report on fixed asset transactions history (i.e., fixed asset movements)	
EGOV/FR/26.111	Generate unposted depreciation calculation report before transferring them to GL but after running depreciation in the assets module	
EGOV/FR/26.112	Asset cost report	
EGOV/FR/26.113	Asset report by major and minor category	
EGOV/FR/26.114	Following activities should generate a report output: - Asset transfer - Asset Disposals - Asset retirement in the form of sale, scrap, write off etc. Asset addition	
EGOV/FR/26.115	Generate automatic reconciliation report for GL and depreciation register	
EGOV/FR/26.116	Retirement Register by month / asset number” - by department - by location/region - by account - by account segment by retirement type	
Management and Cost Accounting **Planning Budgeting Funds and Grants Management**		
EGOV/FR/26.117	Maintain an auditable record of source of funds which can be in the form of Grants, Loans, Equity, Debentures or any other source of funds which be appropriate for RMC.	
EGOV/FR/26.118	Provide the functionality to grant approvals for individual projects and maintain and auditable record of the source of funding for each project	
EGOV/FR/26.119	Maintain of record of the plan versus actual capital expenditure at project level	
EGOV/FR/26.120	Tracking of utilization of funds at project level with multi-level roll-up functionality	
EGOV/FR/26.121	Provide flexibility in reporting for budgeting and variance analysis	
EGOV/FR/26.122	Provide flexibility in reporting of spend and utilization reports	
Management Accounting		
EGOV/FR/26.123	System should have functionality to define internal organization structures for segment reporting and for internal reporting	
EGOV/FR/26.124	Should have functionality to amend organization structure according to business needs with complete audit trail of changes done	
EGOV/FR/26.125	System should have functionality to record business transaction for financial as well as for management account at the same time	
Costing		
EGOV/FR/26.126	Ability to capture and report costs against each dimension in the chart of account structure such as unit, department, location, product, project etc.	
EGOV/FR/26.127	Ability to define cost centres across the organization , including multiple legal entities under a common management control	
EGOV/FR/26.128	Ability to define various elements of costs for cost sheet preparation	
EGOV/FR/26.129	Facility to pool costs and then allocate / reallocate costs to other cost centres / across organization based on predefined basis	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.130	Ability to create flexible cost collectors to collect costs for specific purpose / objective	
EGOV/FR/26.131	Ability to settle such collected cost to another cost centre, asset or WBS element or project	
EGOV/FR/26.132	Ability to print various cost allocation schedules prior to the financial closing of the period	
EGOV/FR/26.133	Ability to allocate overheads either on a percentage basis or as quantified by the service providing department	
EGOV/FR/26.134	Ability to allocate indirect process unit costs to direct process units based on direct cost ratio	
EGOV/FR/26.135	Ability to rerun cost allocations when the underlying data changes	
EGOV/FR/26.136	Ability to combine the costs for several input sources and allocate in one allocation source through parameters	
EGOV/FR/26.137	Ability to allocate common costs across departments/ products / units based on predefined basis.	
EGOV/FR/26.138	Provisions to add relevant taxes and duties wherever applicable	
EGOV/FR/26.139	Facility to reconcile costing reports with financial reports	
EGOV/FR/26.140	Flexibility to accept new detail lines/parameters for preparation of cost sheets	
EGOV/FR/26.141	Ability to derive the costs centres or cost collectors automatically based on the normal accounting postings	
EGOV/FR/26.142	Ability to assign budget for these cost collectors	
EGOV/FR/26.143	Ability to track the actual costs and budget costs on these cost collectors	
EGOV/FR/26.144	Ability to support variance analysis between budget and actual across various periods.	
EGOV/FR/26.145	Ability to set up availability control on these cost collectors and set up warning or error messages when the budget exceeds / matches the actual costs	
EGOV/FR/26.146	Ability to create these cost collectors for reporting purposes only as these costs cannot be allocated further	
EGOV/FR/26.147	Ability to compile the total costs in the primary cost collectors and settle the costs to other cost collectors	
EGOV/FR/26.148	Ability to create various reports about the costs collected in these cost collectors at various time periods and compare them with the budgets	
EGOV/FR/26.149	Ability to compute costs for inventory valuation purpose based on defined accounting policy	
EGOV/FR/26.150	Ability to support categorization of costs into fixed/ variable costs at process/product/cost centre levels or as required by users.	
EGOV/FR/26.151	Ability to accept costs/rates on adhoc basis, where prices have not been finalized.	
EGOV/FR/26.152	Ability to maintain mapping between chart of accounts and costing system along with cost centre/responsibility centre system.	
EGOV/FR/26.153	Ability to allocate cost in the same original GL account Head to multiple cost centres or other cost objects	
EGOV/FR/26.154	Ability to assign Fixed Assets to Cost Centres	
EGOV/FR/26.155	Ability to capture depreciation for cost sheet preparation from the fixed asset module	
EGOV/FR/26.156	Ability to charge of Depreciation to assigned cost centres automatically, while posting Depreciation entries	
EGOV/FR/26.157	Facility to determine cost for any process with or without depreciation and interest component and ability to transfer relevant amount to subsequent process.	
EGOV/FR/26.158	Ability to maintain cost sheets prepared on multiple basis for the same period for comparison purpose.	
EGOV/FR/26.159	Ability to perform Cost allocations (plan/actual cost accounting) based on full costs. Costs are not split into fixed and proportional costs as only a consolidated entry is posted onto the cost collector, for example canteen costs	
EGOV/FR/26.160	Allow to calculates wage costs using the fixed hourly rates determined in cost centre planning	
EGOV/FR/26.161	Allow Standard costing and Marginal Costing	
EGOV/FR/26.162	Ability to do Activity based costing	
EGOV/FR/26.163	Ability to collect actual Labour / factory overheads based on the settings like activity	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	allocations made in the system	
EGOV/FR/26.164	Ability to have Cost Centre Accounting, including itemized costing for specific business events like marketing campaigns or trade fair participation	
EGOV/FR/26.165	Ability to add one or more cost centres or one or more nodes of the standard hierarchy for Cost Centre	
EGOV/FR/26.166	Ability to get the breakup of costs by way of different accounts	
EGOV/FR/26.167	Ability to get itemization or details of the standard cost estimates, where we can get the breakup of costs in the required parameters	
EGOV/FR/26.168	Ability to consider the planned overhead costs in the standard cost estimates based on cost centre planning and activities	
EGOV/FR/26.169	Ability to consider various overheads like material overheads, production overheads and Admin overheads	
EGOV/FR/26.170	Ability to cost roll up from lower levels to higher levels of WBS for Projects	
EGOV/FR/26.171	Ability to maintain cost estimates for materials sent on sub-contracting	
EGOV/FR/26.172	Ability to estimate costs and maintain costs for previous, current and future period in the system	
EGOV/FR/26.173	Ability to cost the subcontracting materials and the status of material lying with Sub-contractors	
EGOV/FR/26.174	Various MIS Reports based on the standard and actual costs and the analysis of variances	
EGOV/FR/26.175	Real-Time Integration of Costing with Financial Accounting	
EGOV/FR/26.176	System should have functionality to manage expenses incurred on work or jobs carried out for internal or external customer	
EGOV/FR/26.177	System should provide functionality to plan internal and external resources for various categories of jobs	
EGOV/FR/26.178	System should allow planning of various types of costs for different categories of jobs	
EGOV/FR/26.179	System should have functionality to keep track of costs and resources consumed on maintenance of internal or customer assets	
EGOV/FR/26.180	System should provide adequate control mechanisms for complete lifecycle management of a job or a work order; should have functionality to approve or reject a particular job or a type of expense for a job	
EGOV/FR/26.181	The module shall have: - Define Chart of Accounts as per the guidelines of NMAM - Maintain Bank Account Details - Maintain Details of Vendors - Budget provisioning – Provision for Original and Revised Budget - Re-appropriation of Budget between accounting heads - Provision to records Receipts - Transfer of Receipts – cash/cheque to Bank Accounts - Record direct debit/ credit to bank accounts in books of accounts - Entry of Bills /Invoice Received from vendors - Authorization of bills as per the work-flow defined - Payment Vouchers once the payment is approved. - Keep track of Cheque books and cheque leaves. - Facility for cheque printing - Direct Payment up to specific limit - Journal Voucher Entry - Authorization of Journal Voucher - Contra Voucher Entry - Reversal of Vouchers - Provision for Bank Reconciliation at any point in time. - Manage Deposits received from vendors, citizens. - Keep track of Grants received and expenses made against the specific grant - Keep record of Investment made and interest accrued on the investments - Loans management Advances management	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/26.182	Books of Accounts and Registers: - Cash Book, Bank Book, Cashier's Cash Book - Ledger – Single or Multiple account heads - Trial Balance, Income & Expenditure, Balance Sheet - Cash Flow Statement - Bill Register - Payment Register - Deposit Register - Investment Register - Loans Register Advances Register	
EGOV/FR/26.183	Provision for defining new cost heads (GL, CC, SL, etc.)	
EGOV/FR/26.184	Defining and configuring budget heads & sub-heads and tagging them with respective section of RDA.	
EGOV/FR/26.185	Entering the forecast details as per the organization standards.	
EGOV/FR/26.186	Provision to define timeline for budget forecast submission date.	
EGOV/FR/26.187	Provision of Voucher configuration screen for regular voucher entries and defining respective voucher types.	
EGOV/FR/26.188	Manage Accounts Receivable and Payables.	
EGOV/FR/26.189	Provision to open accounts and enter transactions as per the standard accounting practice.	
EGOV/FR/26.190	Preparation of the financial statement from transaction like Trail Balance/ Profit & Loss Account/ Balance Sheet as per the standard of the client.	
EGOV/FR/26.191	Provision for uploading Bank Challan Receivable.	
EGOV/FR/26.192	Generation of Costing & Analysis reports is facilitated through the proposed system.	
EGOV/FR/26.193	Provision to enter the different type of taxes and report the tax payment details.	
EGOV/FR/26.194	Provision to generate various accounting reports as per the Organization standard.	
27. Purchasing & Inventory Management		
Purchase Requisition		
EGOV/FR/27.1	Ability to create Purchase Requisitions for goods and services	
EGOV/FR/27.2	Ability of employees (or authorized users) or departments to create requisitions and have visibility of PO's issued against these requisitions	
EGOV/FR/27.3	Ability to convert requisition to request for quotations (RFQ) automatically. RFQ should be attached to selected vendors based on past data/performance	
EGOV/FR/27.4	Ability to consolidate multiple purchase requisition from different departments	
EGOV/FR/27.5	Ability to monitor the status of purchase requisition raised	
EGOV/FR/27.6	Ability to attach documents (e.g. Word, excel, pdf etc.) with the header and lines of purchasing documents (PR, RFQ, Quotes and PO).	
EGOV/FR/27.7	Ability to raise Purchase Requisition against a project	
EGOV/FR/27.8	Ability to raise Purchase Requisition for service contract with vendors	
EGOV/FR/27.9	Ability to automatically create requisition if the quantity on hand goes below re order level	
EGOV/FR/27.10	Approvals of these requisition should conform to the powers vested in signing authorities. Necessary workflows must be available to facilitate approvals on the system	
Receive & Evaluate Quotation		
EGOV/FR/27.11	Ability to prepare Request for Quotation against a purchase requisition	
EGOV/FR/27.12	Ability to electronically send the request for quotation and link it to multiple Bidders	
EGOV/FR/27.13	Ability to enter the quotes received	
EGOV/FR/27.14	Ability to have an expiry date for the Quote	
EGOV/FR/27.15	Ability to Analyse Vendor's Quotations (Technically, Financially) on following criteria - Lowest Price - Best Delivery - By assigning points on quality offered - Payment Term - Landed Cost (Freight etc.)	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Relationship with Vendor (Agent, supplier etc.) - User definable criteria System should be able to evaluate the quotation on the basis of above criteria	
EGOV/FR/27.16	Ability to copy vendor's quotation into PO either as a whole or selected lines	
Purchase Order		
EGOV/FR/27.17	Ability to convert quotation/requisition to purchase order	
EGOV/FR/27.18	Ability to create multiple purchase orders against a single quotation/requisition	
EGOV/FR/27.19	Ability to create purchase order for goods and services	
EGOV/FR/27.20	Ability to create purchase order for service contracts with vendors	
EGOV/FR/27.21	Ability to create long term contracts in the system with either a limit either on time period, quantity or value either a limit either on time period, quantity or value	
EGOV/FR/27.22	Ability to create multiple releases against the long term purchase contracts	
EGOV/FR/27.23	Ability to create replenishment automatically for specific items with respect to the inventory norms defined I.e. safety stock, reorder point, inventory turns	
EGOV/FR/27.24	Ability to enter the PO's in different currencies in the system.	
EGOV/FR/27.25	Ability to record purchase order acknowledgement from vendor	
EGOV/FR/27.26	Ability to enter price, state taxes, central taxes, GST, municipal levies, payment terms, special discounts, delivery instructions, delivery schedule etc. in purchase order/release order	
EGOV/FR/27.27	Ability to set receiving tolerance limits in purchase order or service order	
EGOV/FR/27.28	Ability to set 2/3/4 way matching requirements in the purchase order	
EGOV/FR/27.29	Ability to send approved PO electronically to vendors (Fax, email etc.)	
EGOV/FR/27.30	System should allow reprint of PO with 'copy' marked on the print out	
EGOV/FR/27.31	System should be able to capture information pertaining to freight, insurance, etc. at each line item selection as per the terms (CIF, FOB, etc.)	
EGOV/FR/27.32	Ability to capture penalty clause in PO (% wise, daily rate and lump sum)	
EGOV/FR/27.33	Ability to enter project details while creating purchase order and interface the details to project	
EGOV/FR/27.34	Purchase order processing is part of the procurement of materials and services. Its primary purpose is to convert demands to purchase orders (with or without reference to a contract) or delivery schedules for a scheduling agreement and to monitor the fulfilment of these documents	
EGOV/FR/27.35	MRP requirements linked to business plans and repair and maintenance programs	
EGOV/FR/27.36	Prepare and dispatch RFQs/RFPs/RFIs	
EGOV/FR/27.37	Consolidate discounts across orders under particular contracts	
EGOV/FR/27.38	Consolidate dispatching PO’s and PO lines against vendors	
EGOV/FR/27.39	Requirement to separate out carriage and transport costs	
EGOV/FR/27.40	Requirement to dispatch PO’s via various methods i.e. web, email, fax, post.	
EGOV/FR/27.41	Ability to assign Follow-up dates on purchase orders	
EGOV/FR/27.42	Ability to record Comments for follow up activities	
EGOV/FR/27.43	Ability to track different stages of a purchase order (like - In-progress, approved, rejected, closed etc.)	
EGOV/FR/27.44	Ability to follow up of shipment which are in transit by sea or air	
EGOV/FR/27.45	System should have provision for registration of documents received, awaiting arrival of ship	
Receiving Good/Services		
EGOV/FR/27.46	Ability to receive gods and services against a purchase order	
EGOV/FR/27.47	Ability to record inspection report for items	
EGOV/FR/27.48	Ability to update inventory on item receipt / post-inspection clearance for items with mandatory inspection requirements	
EGOV/FR/27.49	Ability to generate receiving document on receipt	
EGOV/FR/27.50	Ability to receive un-ordered receipts or substitute items with proper authorization as defined by business	
EGOV/FR/27.51	Ability to record multiple receipts against a single PO	
EGOV/FR/27.52	Ability to record serial number, expiry date and batch number during receipt for specific items (tracking item by serial number e.g. meters for water & electric tracking item by serial number e.g. meters for water & electricity)	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/27.53	Ability to record labour hours and material consumed by an internal employee or contractor against a maintenance work order. These entries must reflect in the costs accumulated against a specific work order.	
EGOV/FR/27.54	System should have provision for rejection of unacceptable items with creation of Discrepancy Report	
EGOV/FR/27.55	The solution must accommodate various types of receipt - standard 3-way match, blanket (i.e. limit) order receipting, exemption on receipt for orders up to a specified value. Additionally the user must have an option of a 2 way match where the vendor need not submit an invoice. The payments are cleared by comparing the G/R or service entry sheet against a PO or purchase contract.	
EGOV/FR/27.56	Receiving an Incoming Invoice, The ability to receive, enter, and check vendors' invoices for correctness. The ability to manually enter incoming invoices and automated procedures for creating invoices, such as the automated processing of receipts or goods and services.	
EGOV/FR/27.57	Verifying an Incoming Invoice The ability to check incoming invoices for correctness in terms of their content, prices, state taxes, central taxes, GST, municipal levies and arithmetic, thus defining the basis for the payment run. The price and conditions are compared to the conditions in the purchase order, or the invoiced quantity is compared to the received quantity. If differences exceed user defined limits, the invoice should be blocked automatically for payment. Tax calculation and processing of delivery costs are also to be integrated	
EGOV/FR/27.58	The ability to for one person to process/verify the invoice and another person to approve the processing and processing of vendor invoices is required. Workflow functionality is necessary to control the process.	
EGOV/FR/27.59	Release of Blocked Invoices The ability to release invoices that have been blocked can be released for payment using a monitor function. The ability to automatically release of invoices for which the blocking reasons have been clarified. Workflow features support the release process.	
EGOV/FR/27.60	Requirement to create self-bill invoices against agreements or Contracts from within the solution.	
EGOV/FR/27.61	Requirement to reject invoices if they are not valid or legal documents.	
Maintain Vendor Records		
EGOV/FR/27.62	Ability to maintain the following information per vendor:	
EGOV/FR/27.63	Vendor code	
EGOV/FR/27.64	Vendor name	
EGOV/FR/27.65	Multiple Contact name	
EGOV/FR/27.66	Multiple Vendor address	
EGOV/FR/27.67	P.O. Box	
EGOV/FR/27.68	E-mail address	
EGOV/FR/27.69	Phone number (multiple)	
EGOV/FR/27.70	Fax number	
EGOV/FR/27.71	Default payment / credit term	
EGOV/FR/27.72	Default currency	
EGOV/FR/27.73	Multiple Vendor bank account number	
EGOV/FR/27.74	Default delivery options	
EGOV/FR/27.75	Product Description/category	
EGOV/FR/27.76	ISO Certification & validity	
EGOV/FR/27.77	System to be able to classify vendors as registered/ unregistered and certified/ uncertified, international/domestic.	
EGOV/FR/27.78	System to be able to capture the rules on which the vendor is to be assessed	
EGOV/FR/27.79	Ability to automatically update vendor rating based on pre-defined rule	
EGOV/FR/27.80	Ability to maintain approved supplier lists for inventory items	
EGOV/FR/27.81	Same entity can be both customer and vendor, link to be maintained and referred as related party	
EGOV/FR/27.82	Ability to have vendor specific payment terms	
Approval Hierarchies		
EGOV/FR/27.83	Ability to designate approval hierarchies to approve Purchase Requisitions,	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	Purchase Orders and Vendor Quotations based on the following criteria:	
EGOV/FR/27.84	Amount limit	
EGOV/FR/27.85	Item ranges	
EGOV/FR/27.86	Account Ranges	
EGOV/FR/27.87	Ability to send an electronic notification to approver to take action on the Purchasing document submitted for approval	
EGOV/FR/27.88	Ability to send an electronic notification on approval or rejection of purchasing document (PR, PO and Quotation) to initiator	
EGOV/FR/27.89	Ability to automatically forward document for approval to next person in hierarchy if the document is delayed beyond the specified time with a designation	
Purchasing MIS		
EGOV/FR/27.90	Ability to track the status of PR's with respect to PR log date, Item code, quantity etc.	
EGOV/FR/27.91	Ability to track the status of PO's with respect to PO log date, Item code, quantity and expected time of arrival of the shipment	
EGOV/FR/27.92	Ability to generate report on pending PR/PO supplier-wise, item-wise and department-wise	
EGOV/FR/27.93	Ability to generate report when level stock on-hand below reorder level with information on PO pending, PR pending etc.	
EGOV/FR/27.94	System should have the ability to print summary of expected receipts	
EGOV/FR/27.95	Ability to print purchase register for the month	
EGOV/FR/27.96	Ability to generate reports on documents pending for approval on which no action has been taken for more than N number of days.	
EGOV/FR/27.97	Ability to inquire / report on the item purchase cost history over a user defined date range	
EGOV/FR/27.98	Ability to generate receipt register	
EGOV/FR/27.99	Ability to perform ageing analysis for outstanding Purchase Orders based on cost centre, vendor etc.	
EGOV/FR/27.100	Functionality to generate statutory reports/returns as required by state government for filing sales tax and/or excise duty returns	
Maintain Inventory Items		
EGOV/FR/27.101	Ability to setup and maintain item codes with different segments	
EGOV/FR/27.102	Ability to maintain the following information for items but not restricted to:	
EGOV/FR/27.103	Item code	
EGOV/FR/27.104	Item description	
EGOV/FR/27.105	Purchase lead time per item / supplier	
EGOV/FR/27.106	Vendor item code	
EGOV/FR/27.107	Default purchasing unit of measure	
EGOV/FR/27.108	Minimum stock level	
EGOV/FR/27.109	Item Status (Active, Obsolete, Blocked etc.)	
EGOV/FR/27.110	Expiry Date	
EGOV/FR/27.111	Serial Number and Batch Number (for serialized inventory tracking and batch tracking)	
EGOV/FR/27.112	Barcode	
EGOV/FR/27.113	Ability to group items into categories and sub-categories	
EGOV/FR/27.114	System to be capable of linking the supplier item code with the item code in the item master	
EGOV/FR/27.115	Ability to maintain conversions between units of measure	
EGOV/FR/27.116	System should have provision for serial-number control of items	
EGOV/FR/27.117	System must support bar coding and have the ability to scan pre-printed form containing bar codes, quantities, and item descriptions	
EGOV/FR/27.118	Ability to maintain catalogs item-wise and supplier-wise	
EGOV/FR/27.119	Ability to update catalogs periodically through catalog imports	
Locations		
EGOV/FR/27.120	System should support creation of multiple warehouse locations and attach type/ categories of transactions which the warehouse locations can support	
EGOV/FR/27.121	System should have the ability to support warehouse area classification	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/27.122	Ability to categorize locations and assign items to locations	
Maintain Kits		
EGOV/FR/27.123	Ability to define bill of materials/Kits	
EGOV/FR/27.124	Ability to explode bills and transfer individual items to Inventory	
EGOV/FR/27.125	Ability to combine individual items and issue the master item	
Maintain Stock Levels		
EGOV/FR/27.126	Ability to maintain minimum stock levels for items	
EGOV/FR/27.127	Ability to generate alerts if the quantity falls below pre-defined limits	
EGOV/FR/27.128	Ability to allow negative stock for specific items and record appropriate costing entries	
EGOV/FR/27.129	Ability to classify items based on ABC classification. ABC classification should be based on value of stock & value of movement within a year	
Item Costing		
EGOV/FR/27.130	Supports the following costing methods:	
EGOV/FR/27.131	Standard	
EGOV/FR/27.132	FIFO/LIFO	
EGOV/FR/27.133	Weighted average	
EGOV/FR/27.134	Ability to track the item cost for all material transactions	
Transactions		
EGOV/FR/27.135	Ability to define transaction types and set pre-defined rules for each transaction type	
EGOV/FR/27.136	Ability to issue items against:	
EGOV/FR/27.137	Internal Requisition (IR)	
EGOV/FR/27.138	Maintenance Work Order	
EGOV/FR/27.139	Material requisition from projects	
EGOV/FR/27.140	Ability to generate pick-lists for all material issue	
EGOV/FR/27.141	Ability to generate pick list sequentially. (If the store-keeper goes to a particular area system should give all items to be picked from that area)	
EGOV/FR/27.142	Ability to print location information on pick-slip	
EGOV/FR/27.143	Ability to inspect items on receipt	
EGOV/FR/27.144	Ability to Record quality issues and defect if any	
EGOV/FR/27.145	Ability to scan and record barcode information at the time of receipt	
EGOV/FR/27.146	Ability to upload Goods receipts voucher details from excel to the system.	
EGOV/FR/27.147	Ability to record items returned from Projects to Inventory	
EGOV/FR/27.148	Ability to provide provision for ageing inventory	
Monitor Ageing Stock		
EGOV/FR/27.149	Ability to generate stock aging report based on the receipt date by:	
EGOV/FR/27.150	Aging slots (in days)	
EGOV/FR/27.151	Item-wise	
EGOV/FR/27.152	Category-wise	
EGOV/FR/27.153	Ability to generate stock ageing analysis based on the receipt date	
Physical Inventory & Cycle Counting		
EGOV/FR/27.154	Ability to generate count sheets based on user defined criteria:	
EGOV/FR/27.155	Quantity, e.g. include items with quantity above 10 pieces	
EGOV/FR/27.156	Value, e.g. include the items with unit value above 50K	
EGOV/FR/27.157	Item Category	
EGOV/FR/27.158	Location	
EGOV/FR/27.159	Ability to sort the count sheets by:	
EGOV/FR/27.160	Item	
EGOV/FR/27.161	Location	
EGOV/FR/27.162	Shelf / bin number	
EGOV/FR/27.163	Ability to perform a re-count if the stock difference is beyond pre-defined limits	
EGOV/FR/27.164	Ability to identify the type of physical count adjustments as:	
EGOV/FR/27.165	Shortage / Excess	
EGOV/FR/27.166	Damaged (With percentage damage)	
EGOV/FR/27.167	Non usable items (scrap)	
EGOV/FR/27.168	Ability to monitor the items as count in progress, completed etc.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/27.169	Ability to define the cycle count frequency per item, e.g. every 30 days	
EGOV/FR/27.170	Ability to freeze normal inventory transactions during physical count	
EGOV/FR/27.171	The system should post the stock adjustments only after approval in system	
Forecasting		
EGOV/FR/27.172	Ability to perform min-max and re-order point planning	
EGOV/FR/27.173	System should have the provision for using standard Inventory forecasting techniques	
Inventory MIS		
EGOV/FR/27.174	Ability to report the transaction statistics by type (e.g. number of receipt transactions, shipments, transfers, returns etc.) by product group and month	
EGOV/FR/27.175	Ability to generate material transaction register	
EGOV/FR/27.176	Ability to generate item movement report to track all transactions based on following criteria	
EGOV/FR/27.177	Period-wise	
EGOV/FR/27.178	Item-wise	
EGOV/FR/27.179	Category-wise	
EGOV/FR/27.180	Transaction type wise	
EGOV/FR/27.181	Ability to generate damaged stock report	
EGOV/FR/27.182	Ability to generate stock expiry report period-wise	
EGOV/FR/27.183	Ability to track items reserved with reference	
EGOV/FR/27.184	Ability to track slow moving items based on following criteria	
EGOV/FR/27.185	Percentage movement	
EGOV/FR/27.186	Period-wise	
EGOV/FR/27.187	Item-wise	
EGOV/FR/27.188	Category-wise	
EGOV/FR/27.189	Transaction type wise	
EGOV/FR/27.190	System needs to provide a report at the end of each physical inventory/cycle counting/perpetual stock count indicating product category wise, item-wise, location wise, period-wise variances between the actual physical stock and stock in the system	
EGOV/FR/27.191	Ability to generate report on ABC classification based on stock value and movement in a year	
EGOV/FR/27.192	Ability to generate report on inventory balance on-hand with GRV details	
EGOV/FR/27.193	Non-moving items for a selected period detailing complete history from receipt until the last issue	
28. e-Procurement		
General		
EGOV/FR/28.1	The system must be able to log all the activities carried out on the system by any user.	
EGOV/FR/28.2	The administrator shall be able to make intelligent search on the log based on user name, time period, type of activity, etc.	
EGOV/FR/28.3	Audit trail of the entire system operations shall be maintained in secured environment.	
EGOV/FR/28.4	The E-Procurement system should adhere to stringent security norms like SSL, firewall and other security guidelines	
EGOV/FR/28.5	E-Procurement system will have native integration with back-end functionalities for operational procurement, inventory management.	
EGOV/FR/28.6	E-Procurement system will be capable to handle both materials and services	
EGOV/FR/28.7	The solution should have comprehensive business workflow engine to create and manage different kind of workflow requirements triggered by specific events.	
EGOV/FR/28.8	E-Procurement system should have comprehensive functionality for supplier evaluation	
EGOV/FR/28.9	Supplier evaluation can be done based on past purchase transactions considering different parameter like price, quality, delivery, services etc. The score of these parameters could be calculated automatically by the system or entered manually.	
EGOV/FR/28.10	System will have provision to conduct supplier evaluation based on feedback from business users through questionnaire. The questionnaire can be triggered on	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	specific events automatically by the system or by conducting a web-based survey.	
EGOV/FR/28.11	It shall have standard reporting formats available. Reports shall be available in these standard formats at any given time.	
EGOV/FR/28.12	The system must provide detailed drilled down reports.	
EGOV/FR/28.13	The system must enable user to configure/develop reports on different parameters for trend analysis, reports on supplier participation etc.	
EGOV/FR/28.14	Management of user IDs and password and setting up hierarchy levels and role definitions for different users.	
EGOV/FR/28.15	The system must provide a supplier administration module to add, delete, enable or disable the suppliers or supplier group.	
EGOV/FR/28.16	The system must provide for reports in both flat file and Excel formats.	
EGOV/FR/28.17	The E-Procurement system should have document collaboration facility among Client, bidders and suppliers. They should be able to share documents in a secured manner online. The upload, download and storage of the documents would be folder-based and easy-to-use.	
EGOV/FR/28.18	The solution will have in-built capability to create purchasing documents, legal contracts with clauses, terms & conditions etc. and stored in a structured manner. The output could be PDF MS Word or XML file.	
EGOV/FR/28.19	Facility for empanelment/registration of suppliers on the portal	
EGOV/FR/28.20	Provision to create different questionnaire for different product categories and services	
EGOV/FR/28.21	Supplier will be able to register or apply for certain product or services themselves over internet by entering/answering basic questions.	
EGOV/FR/28.22	Based on supplier selection or application, a questionnaire can be sent to supplier in a secured manner to get more information	
EGOV/FR/28.23	The quotations can be categorized.	
EGOV/FR/28.24	Questions can be answered through texts, checkboxes, yes/no with validity.	
EGOV/FR/28.25	Designated person can check and review answers of the questions and then approve or reject the registration request.	
EGOV/FR/28.26	There will be supplier directory to check different supplier with their statuses	
EGOV/FR/28.27	Potential suppliers can be confirmed to be supplier of materials or services	
EGOV/FR/28.28	Supplier will receive administrative login and password information so that they can maintain their own information online	
EGOV/FR/28.29	After approval, supplier will be able to get notification for tenders, purchase order etc. to collaborate with Client	
EGOV/FR/28.30	Suppliers will get administrative role to create other user ids for their organizations to carry out different purchasing activities according to different roles.	
E-Tendering		
EGOV/FR/28.31	Employees will be able to raise purchase request themselves or on the behalf of other employee	
EGOV/FR/28.32	Solution should have the capability of team purchasing where they can do all the sourcing activities as a team and collaborate	
EGOV/FR/28.33	The system shall be capable of handling limited tenders, open tenders, global tenders, rate contract, reverse auction etc.	
EGOV/FR/28.34	There shall be no limit with the system in terms of interacting with Payment Gateways for purpose of financial transactions.	
EGOV/FR/28.35	E-tendering system will support complex service procurement where service can be defined in a multi-level service hierarchy with defined value limit	
EGOV/FR/28.36	For each type of payment, the work flow for making payment shall be part of the process. For example, if vendor has to make payment for tender form, the web page where tender forms are listed shall guide the user to make payment. Once the vendor chooses to pay he shall be taken to the payment gateway and payment shall be accepted.	
EGOV/FR/28.37	System shall be capable for adoption for supporting different kind of formats of tenders, tender conditions and output reports as defined by the Client	
EGOV/FR/28.38	The base currency of the System must be Indian Rupees. The currency shall be customizable/configurable in case of global tenders.	
EGOV/FR/28.39	The system must allow Users to locate tenders quickly through on-line search	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	facilities in a variety of ways including tender no, generic descriptions, etc.	
EGOV/FR/28.40	The system should provide the following bid stages in the tendering process: - Pre-Qualification bid stage - Technical bid stage - Reverse auction - Price/commercial bid stage Single stage, techno-commercial bid stage	
EGOV/FR/28.41	System should be configurable to create various types of users as mentioned below: - Authorized personnel from Client for access and use of the different modules of the system like NIT, bid preparation, bid evaluation etc. - Authorized personnel from the bidder organizations - System Administrators - Super user to control all operations on the e-Procurement Portal; and Any other user such as payment gateway providers or as per the architecture of the proposed solution by the vendor / consortium.	
EGOV/FR/28.42	Secured electronic alert facility to the registered suppliers on the portal, whenever a new tender / corrigendum / addendum is published.	
EGOV/FR/28.43	Search facility for the tender floated on the web site category wise, tender no wise etc.	
EGOV/FR/28.44	Users shall enter the quantity required for tendering directly into the tender based on manual inputs received by them. On receipt of indent for a particular item, the user shall initiate the preparation of tender document along with technical requirements, payment terms, Schedule of requirements, price schedule etc.	
EGOV/FR/28.45	The tender document shall be prepared online. These shall be a provision to prepare each section, for example special conditions, functional requirement if any, schedule of requirements, price schedule, technical specification etc., separately by different users assigned by administrator.	
EGOV/FR/28.46	There shall be a work flow to get the prepared tender document approved online by the concerned section users for the purpose of floating same by the concerned procurement wing.	
EGOV/FR/28.47	The officers in the approving chain shall be able to view the tender document and place his remarks in the space provided for the purpose. These remarks and suggested changes shall be viewable to the user who prepared the document. He shall be able to imbibe these comments in to the tender document online.	
EGOV/FR/28.48	There shall exist a facility to authorized personnel of supplier organizations for - Online downloading of Complete Tender Documents, multiple Addendum and multiple corrigendum with online payments or offline payments received through demand drafts. Activation of Online/Offline payments modes shall be configurable.	
EGOV/FR/28.49	The GUI of the system shall have a tender designing facility. Designing of tender documents for different types of tenders such as EOI (expression of interest), Limited Tender, Advertised Tender, Global Tender both for works, consultancy and supply of goods and services shall be possible so as to include existing features of submission of bids with complete break up indicating basic rate, excise duty, sales tax/VAT, packing, forwarding, freight etc., with supply to multiple consignees.	
EGOV/FR/28.50	As and when addendum or corrigendum is posted, all suppliers who have officially procured tender document online should receive automatic online reminders through registered emails.	
EGOV/FR/28.51	The relevant approving authority should get an email alert whenever any tender has come to him/ her for approval.	
EGOV/FR/28.52	NIT shall be visible to users of in the approval hierarchy: The NIT approver should have the following functionalities: Approve the NIT, Reject the NIT, Route the NIT to a specific person for review, Insert comments	
EGOV/FR/28.53	For creation of NIT there shall be a proper approval process which may involve many users who are in a hierarchy. The transactions and remarks of such users shall be visible to all users in the same hierarchy. On final approval, already configured for each hierarchy, notice/message shall go the user who initiated the process.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/28.54	The NIT/Tender creator should be able to select any combination of these stages to create a single stage or two stage or 3 stage tender.	
EGOV/FR/28.55	A provision shall exist to take a print out or send mail to approved print media addresses in a predefined format.	
EGOV/FR/28.56	The System must provide the facility to publish the NIT on its web interface for public. The link for website shall be provided in official website also.	
EGOV/FR/28.57	On publication of the tender, the system should generate an email/SMS alert to the registered suppliers and concerned company users.	
EGOV/FR/28.58	It should be possible by configuration to have a copy of the Tender Document for free online viewing by prospective suppliers.	
EGOV/FR/28.59	The official copy of the Tender Document downloaded online after making the necessary payment, if any, (online or offline) should have a unique reference number such that these are not transferred to other Suppliers	
EGOV/FR/28.60	There should be facility for re-bidding for one or more bid parts without having to re-float the whole tender.	
EGOV/FR/28.61	The System must allow tenders to be tracked through their lifecycle, providing visibility of tender status, user comments and responses, evaluation & decision history, etc.	
EGOV/FR/28.62	The system shall have pre-bid queries/clarification functionality.	
EGOV/FR/28.63	The system should allow for issue of corrigendum's/amendments to be published on the E-Procurement site.	
EGOV/FR/28.64	The system should be able to send an alert to the concerned vendors.	
EGOV/FR/28.65	All such corrigendum's/amendments shall become the part of the tender on closing of the tender and shall be viewable accordingly.	
EGOV/FR/28.66	The bids, during submission, shall be encrypted using public keys of vendor. The opening of the submitted bids shall only be possible through private keys of the vendor either from his remote position or being present physically at company's location for tender opening. The same process shall be repeated for all the bids of different vendors.	
EGOV/FR/28.67	The vendor shall be allowed to revise his bid before due submission date of the bid as defined in the tender document. Only the last bid submitted by the vendor shall be considered by the system.	
EGOV/FR/28.68	The company users should have the facility of digitally signing the documents while issue of clarifications or any document issued to the bidders post or pre tender submission. For this purpose, bidders shall receive notification for any notice issues for tender clarification, addendum or corrigendum.	
EGOV/FR/28.69	After the submission of bids, it shall not be possible to change anything in the bid from either side. Bidder shall explain this feature in the bid response. The same process shall also be mentioned in the help menu of the portal.	
EGOV/FR/28.70	The system shall ensure secured flow of content and delivery of the messages with different users.	
EGOV/FR/28.71	It shall be possible to submit Bids, online, in single or multiple stages such as pre-qualification, technical and financial bids as specified in the respective tender or as per the procurement policy decisions.	
EGOV/FR/28.72	The bid submission process shall be designed in such a way that all required documents (pre-configured) and bid components shall be uploaded at the time of bid submission. In case any document is not uploaded, the bid submission process shall not be completed. The mandatory documents shall be indicated by the user uploading the tender by way of marking/ on various options during the tender preparation.	
EGOV/FR/28.73	It shall be possible that all key parameters of technical bids are filled by the bidders in a pre-defined format. The system shall have provision to allow any additional information/document that the prospective bidder may like to submit as part of the bid submission. Attachment feature needs to be provided for submission of documents.	
EGOV/FR/28.74	For financial bids, it shall be submitted in a pre-defined format. All the mandatory fields in the financial bids shall be filled without exception. Bidder shall not be allowed to progress further in case he/she leaves a field unfilled.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/28.75	Apart from listed items in financial bid, the vendor shall be allowed to insert additional items which he/she wants to quote as part of bid. Separately he/she shall also be allowed to give breakup cost of line items if required.	
EGOV/FR/28.76	It shall be possible to view the submitted bids in a consolidated fashion to both the bidder and RMC in a pre-defined format. The summary of bids shall be viewable to the bidder when they are submitting the bid and to RMC users when the bids are being opened.	
EGOV/FR/28.77	For the financial portion of the bid, it shall be possible to submit the name of the product, quantity offered, unit price, different taxes applicable, discounts offered and the total price, etc.	
EGOV/FR/28.78	The bidder shall be given the option to insert additional fields in the financial bid form to insert any additional levies/taxes to cater to extra ordinary charges/levies.	
EGOV/FR/28.79	For global tenders it should be possible to submit price-bids in prescribed Foreign currency as specified.	
EGOV/FR/28.80	All the received bids shall be stored in an encrypted form in an Electronic Secure tender box. These bids shall be time stamped and entire process shall be highly secure. It should not be possible to open and view the contents of the Electronic Secure Tender Box till the specified time has elapsed.	
EGOV/FR/28.81	Facility shall be available to the authorized users to login simultaneously within a defined period to open technical bid and price bid. All the designated persons need to be logged in within the time period and open the bid. Bid administrator will be able to assign technical bid and price bid openers in a tender.	
EGOV/FR/28.82	The System must not allow Users from viewing the bids before the tender opening date & Time.	
EGOV/FR/28.83	System should have the capability to involve internal and external experts for online bid evaluation	
EGOV/FR/28.84	Experts will be able to provide their score and comments online	
EGOV/FR/28.85	The comparative sheet of the price bids along with the technical bid details shall automatically get transferred to the Evaluation Committee members, whose email id shall be predetermined and configured in the system.	
EGOV/FR/28.86	The System must automatically process and save the bid evaluation results in a specified folder. Authorized users, including the Evaluation Committee members shall be allowed to view and evaluate the bidders' responses against the parameters specified and attach evaluation results to the bids with their comments. These comments shall not be visible to users other than the evaluation committee members. Each tender may have specific and unique evaluation group.	
EGOV/FR/28.87	For Price-bids of global tenders, it shall be possible to prepare related comparative charts in the offered foreign currency converted to INR as per the conversion factor defined. If the conversion factor has not been defined earlier at the NIT stage, then before opening of the comparative chart the system shall prompt the user to enter the necessary conversion factor.	
EGOV/FR/28.88	After evaluation process is over, the bid documents shall be stored in a secure manner with use of digital signatures etc. No tempering of these stored bids shall be possible as they may be required to be produced legally on a later date.	
EGOV/FR/28.89	The System must support separate workflows for Pre-Qualification, Technical, Commercial and Techno-commercial evaluation stages.	
EGOV/FR/28.90	For each stage of evaluation, the approver shall have the following functionalities: Approve the evaluation of the evaluator, Route the Evaluation to a specific person for view and comment either within the department or sub-department or between different departments, evaluation report	
EGOV/FR/28.91	Facility shall exist to prepare the report of the evaluation committee with the help of pre designed templates. The report shall be submitted through an online approval process in a desired/configured hierarchy.	
EGOV/FR/28.92	The facility shall exist for preparation of online contracts/P.O.s with basic formats readily available in the system. It shall be possible to insert any product specific conditions through a separate link or drop down menu or any other means so as to insert the same in the contract.	
EGOV/FR/28.93	Provision of awarding contract to one or more bidders based on tender conditions	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	after proper approval through online approval process as in other modules of this tender. The parameter and percentage of quantity to each vendor shall be pre-defined at the time of NIT preparation.	
EGOV/FR/28.94	Create, approve and dispatch intimation of acceptance of tender for successful bidder and unsuccessful bidders.	
EGOV/FR/28.95	Create & Dispatch of purchase order to the selected single Suppliers	
EGOV/FR/28.96	Create & Dispatch of split/part purchase orders to the selected Suppliers.	
EGOV/FR/28.97	System should have provision to process tender fee. Bidders should be able to pay tender fee online	
EGOV/FR/28.98	Solution should have capability to handle EMD (Earnest money deposit) or Bank Guarantee) and Performance Bank Guarantee. Auto monitoring of expiry dates is required for Bank Guarantees.	
EGOV/FR/28.99	Solution should be able to manage waiver of EMD or tender fee.	
29. Contracts Management		
EGOV/FR/29.1	The contract management solution should facilitate searching and managing contractual as well as financial data flow.	
EGOV/FR/29.2	Template based Contract development process	
EGOV/FR/29.3	Enhanced Contract reviews to reduce risk and enhance predictability, help business achieve higher profits in terms of time, money, stakeholder's satisfaction	
EGOV/FR/29.4	Standardization across contracts across organisation	
EGOV/FR/29.5	Build Contracts basis prior experiences by applying learning through predictive & intelligent technology-led methodologies	
EGOV/FR/29.6	Reduced turnaround time to review Contracts with better consistency to provide better support to business	
EGOV/FR/29.7	Digital repository of contracts throughout lifecycle to develop & leverage knowledge	
EGOV/FR/29.8	Online legal support from experts to support RMC team on various aspect throughout Contract Lifecycle Management	
EGOV/FR/29.9	Fewer people deployment	
EGOV/FR/29.10	Capture and active management of contract master data of - any form main, individual and collective contracts, addendums, etc. - any type sales, purchase and rental contracts, service agreements, memberships, warranties, etc. - any category or type vendor and customer contracts, internal agreements, etc.	
EGOV/FR/29.11	Document management centre for all types of documents (documents stored in an optical archive and PC documents), Mails, internal notes and URL links	
EGOV/FR/29.12	Tracing and alerts management for key dates as terms of notice, renewal dates and other terms or due-dates	
EGOV/FR/29.13	Assignment of partners and contacts to predefined roles	
EGOV/FR/29.14	Customizable contract status management	
EGOV/FR/29.15	Activity and Task management	
EGOV/FR/29.16	Free definable user fields by contract types	
EGOV/FR/29.17	Form / template based printouts	
EGOV/FR/29.18	Data change history management (contract versioning, change documents, etc.)	
EGOV/FR/29.19	Ability to adapt the user interface on contract type level by customizing	
EGOV/FR/29.20	The contract management solution should integrate seamlessly with the overall solution. The existing user authorization elements should be reused and tightly integrated.	
EGOV/FR/29.21	The platform should be scalable to handle the load of an enterprise-wide contract management approach for RMC and RSCL	
30. Operations, Maintenance and Asset Lifecycle Management		
Properties, Roads, Pipeline, Fibre Network		
EGOV/FR/30.1	Complaints received from the grievance redressal module will need integration to this module.	
EGOV/FR/30.2	Functionality is required to define a location which is a logical representation in the package, that would represent a property or physical location where any equipment such as meter, value, transformers, switches are installed. A location may also represent a road or a channel where a pipeline is housed.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/30.3	Functionality to map the properties and plots in ROURKELA to a location in the package with the facility of external and internal number ranges	
EGOV/FR/30.4	Functionality for mapping roads on to location in the package which has linear characteristics	
EGOV/FR/30.5	Functionality for mapping fibre network channels on to location in the package which has linear characteristics	
EGOV/FR/30.6	Functionality for mapping pipelines on to location in the package which has linear characteristics	
EGOV/FR/30.7	Facility to hierarchically structure the locations in the package with no limitations on depth of the hierarchy. This facility is required for mapping of land parcels or plots as per a location or colony in ROURKELA. Additionally in a plot the location which would house the meter or the valve would also be at a hierarchical level below the plot	
EGOV/FR/30.8	Facility to specify the Geographical Co-ordinates for each location	
Equipment Master		

EGOV/FR/30.9	Equipment Master should capture the following information:
	- Equipment ID (With intelligence built in the code)
	- Manufacturer
	- Supplier (if Different from Manufacturer)
	- Serial number
	- Date of (Purchase, Manufacture, Installed, Overhauled etc.)
	- Equipment / Component Hierarchy (e.g.: An electric motor can be a component of a major equipment)
	- Warranty information (timeframe, conditions, company through which the warranty is held, expiration date)
	- Functionality to define common Faults / Equipment
	- Functionality to link or attach manuals, operating procedures, graphs and other files to equipment
	- Installed by
	- Associated cost, histories and failures of a serialized piece of equipment as it moves throughout a plant or facility
	- Functionality to track time-related information for Piece of Equipment based on parent Equipment
	  - Time since new (TSN)
	  - Time since overhaul (TSO)
	- Functionality to input and track location of the Equipment / Components
	- Functionality to define multiple maintenance organizations within the company
	Functionality to define list of spares required for an equipment	

Resource Master		
EGOV/FR/30.10	Functionality to record the details of maintenance engineers / technicians	
EGOV/FR/30.11	Functionality to record skill sets against the employee record	
EGOV/FR/30.12	Functionality to maintenance groups to assign responsibility of the equipment	
EGOV/FR/30.13	Functionality to maintain hourly rates for resources	
Preventive / Predictive Maintenance		
EGOV/FR/30.14	Functionality to create preventive / predictive maintenance schedules for all the equipment.	
EGOV/FR/30.15	Functionality to create preventive / predictive maintenance schedules for all the locations as logically defined in the system	
EGOV/FR/30.16	Functionality to create preventive / predictive maintenance schedules for linear assets and their associated locations as represented in the package	
EGOV/FR/30.17	Functionality to prepare preventive / predictive maintenance check sheets for each equipment / component. Predictive maintenance check sheets should have provision to record discrete values (E.g.: Current, Temperature, Vibration etc.)	
EGOV/FR/30.18	Functionality to define tolerance limits for key parameters like current, temperature etc. The limits should be equipment / component specific	
EGOV/FR/30.19	System should have functionality to provide planned costs for all the planned work based on maintenance schedules	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/30.20	System should have necessary provisions to use master data properties to arrive at the planned costs and also must have integration with financials for reporting of both planned and actual costs	
EGOV/FR/30.21	Functionality to create preventive / predictive maintenance schedules based on any of the following parameters: Operating hours (E.g.: For every 5000 hrs.) Time based (E.g.: Daily, Weekly, Bi-Weekly, Monthly, Quarterly, Yearly etc.) Combination of Operating hours / time (whichever comes first) User defined rules (E.g.: If the observations of predictive maintenance are beyond acceptable limits, new preventive maintenance can be scheduled)	
EGOV/FR/30.22	Functionality to designate a parent / child relationship based on type of maintenance (E.g.: Changing a pump requires various other maintenance operations to be performed)	
EGOV/FR/30.23	Functionality to automatically generate work orders based on the preventive / predictive maintenance schedule	
Notifications		
EGOV/FR/30.24	System should have functionality to create notifications for planned and unplanned work	
EGOV/FR/30.25	System should allow creation of notification from multiple sources e.g. from portal / apps etc.	
EGOV/FR/30.26	System should have capture the details of the complainant in case of reactive maintenance	
EGOV/FR/30.27	System should have necessary functionality to capture the status of the service requests	
EGOV/FR/30.28	System should maintain a complete audit trail from registering of an incident to its conclusion	
Work Orders		
EGOV/FR/30.29	Functionality to generate notifications and/or work orders for the following types of maintenance - Breakdown Maintenance - Preventive Maintenance - Predictive Maintenance - Incident Management - Inspection - Calibration / Testing Others (Modification, Major Overhaul, Design upgrades etc.). The user should be able to define the notification types	
EGOV/FR/30.30	Functionality is required for managing Incidents like a Burst Water Mains, Major Fire or Power Break Down. Announcements and Messaging on Bulletin Boards would be required. Additionally multiple citizens may call regarding the same incident, resulting in multiple work orders being raised thereby unnecessarily flooding the maintenance teams with work. In such an emergency situation the system should prevent duplication of work orders.	
EGOV/FR/30.31	The system should allow creation of a planned as well as reactive maintenance work orders for a location as represented in the package	
EGOV/FR/30.32	The system should allow creation of a maintenance work order for a linear assets and its associated locations as represented in the package	
EGOV/FR/30.33	Automatic notification and/or work order creation for alarms raised via the SCADA system. If necessary the MSI may have to develop a real time interface to achieve this functionality.	
EGOV/FR/30.34	Automatic notification and/or work order creation if a user raises any problem with a RMC asset like a street light through the portal. If necessary the MSI may have to develop a real time interface to achieve this functionality.	
EGOV/FR/30.35	Automatic notification and/or work order creation if a customer services representative in the call centre raises any problem with a RMC asset like an open manhole or pot-hole in the road through the portal. If necessary the MSI may have to develop a real time interface to achieve this functionality.	
EGOV/FR/30.36	System should be capable to accept breakdown requests through any means with	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	complete status tracking of these work orders till resolution via the Portal. There would instances where the work order is outsourced to a vendor or 3rd party for resolution.	
EGOV/FR/30.37	Drill down functionality is also required at work order level to verify the status of each task or operation which are included as a part of the work order	
EGOV/FR/30.38	Functionality to have workflow routing for work orders	
EGOV/FR/30.39	Functionality to track the status of a work order. System should be able to support the following status - Initiated / Waiting for Approval / Prepared / Planned - Waiting for material - Released / open (equipment down) - Completed / Cancelled Soft Closing / Finally Closed	
EGOV/FR/30.40	Functionality to include the following information in work orders - Work Order Start and End Date - Type of work order (preventive maintenance, predictive maintenance, breakdown maintenance etc.) - Type of work (electrical, mechanical, etc.) - Equipment identification and description - Priority (E.g.: Urgent, Normal etc.) - Designated duration of work order (start/end date and time in minutes) - Where was work performed (location, site) - Nature of the problem - Customer (requestor) and method of contact - Date of (Problem reported, work completed etc.) - Resources required (labour, materials, equipment and tools) - Resource ID numbers - Resource availability - Lockout / tag-out procedures - Required permits - Testing requirements (to validate repair) - Detailed work plan (task sequencing and trade dependencies) - Fully integrated real time capture in the work cost details: Actual usage (labour time by employee id, parts, equipment time, time to complete and date completed). Out of the box functionality is also required to periodically review the work orders for allocation of overheads and settlement of variances. - Description of actual work performed - System should have functionality to create quotations for the work that need to be charged to customer. Should be able to produce an itemized quotation - System should have provisions to proceed or not to proceed with quotations depending upon customer's decision - Should have functionality to bill the customer for services rendered and material consumed, must produce an itemized bill - Equipment issues - Equipment condition - Cause of problem - Test results - Date and explanation of past work done on the equipment (type of work, nature of the work, completion time, employees who participated in the work) Prepared by	
EGOV/FR/30.41	Functionality must be there to manage the warranty aspects of an equipment or any component or any spare part used in an equipment	
EGOV/FR/30.42	System should have functionality to track components/ spares used in an equipment with details like serial number/ manufacturer etc. and must have functionality to manage any component / spare part movement with complete audit trail	
EGOV/FR/30.43	Functionality to capture maintenance cost details like labour, costing of materials,	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	services, overhead etc. (external or hired labour, specific maintenance group, etc.)	
EGOV/FR/30.44	Functionality to compare the actual labour hours entered by the technician to the standard labour hours estimated to accomplish the work	
EGOV/FR/30.45	Functionality to calculate labour costs based on type of hours worked (regular, overtime, periodic, corrective, breakdown, reactive, equipment modification, etc. by target rate)	
EGOV/FR/30.46	Functionality to automatically generate notifications/work orders based on the preventive / predictive maintenance schedule	
EGOV/FR/30.47	Functionality for configuration of a work order type, without any source code change of the package	
EGOV/FR/30.48	Functionality to create work orders with varying work order types depending on the nature of the customer grievances or calls.	
EGOV/FR/30.49	Functionality of automatic integration of the Customer Services Portal to maintenance notification and/or work order creation	
EGOV/FR/30.50	System should have provision to print notification / work orders with detailed instructions for delivery of the job	
EGOV/FR/30.51	System should have functionality to update customer about the progress of the job and information may be transmitted by different modes e.g. updates on portal or SMS or Status update on APP	
Maintenance History Management		
EGOV/FR/30.52	Functionality to track general maintenance history data: - By Equipment Identification number, work order number etc. - By Location where service was done By Maintenance Sections involved in the service	
EGOV/FR/30.53	Functionality to use maintenance history to assist in maintenance projections (i.e. resource usage during peak times)	
EGOV/FR/30.54	Functionality to track spare parts consumed against an equipment	
EGOV/FR/30.55	Functionality for automatic updation of maintenance history for an equipment or location (as represented in the system) by a work order.	
MIS		
EGOV/FR/30.56	Functionality to generate downtime report with the following details - Equipment details - Reason for failure - Corrective action taken - Spares consumed Work-order details	
EGOV/FR/30.57	Functionality to generate downtime reports - Equipment-wise - Location-wise Year to date	
EGOV/FR/30.58	Functionality to generate reports on the following for each equipment - Mean Time Between Failures (MTBF) Mean Time to Repair (MTTR)	
EGOV/FR/30.59	Functionality to generate following reports for maintenance - Number of work orders issued and closed per month - Types of work orders opened and closed per month - Number of work orders generated per department - Number of work requests awaiting approval (total, by work order owner and by department whose approval has not been received) - Regular versus overtime hours - Planned versus unplanned costs, hours, usage, etc. - Downtime of equipment per work order, year to date, previous year, etc. - Effective production hours per day - Cost rates by resources - Cost by work type - Maintenance schedule compliance as a percentage of maintenance planned or scheduled jobs completed in a month	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Number of work orders generated from PMs - Maintenance cost / Actual cost comparison for each equipment - Productivity measurement of manpower - Should have functionality to roll up planned / actual costs / planned hours/ actual labour hours consumed by different organization entities other than work order e.g. by department owning the asset. Must have functionality to link technical assets with financial assets to provide asset lifecycle including non-cash expenses like depreciation	
Movable and Non-movable Assets		
EGOV/FR/30.60	Defining IT and not-IT asset master.	
EGOV/FR/30.61	Codification of assets as per the organization standards.	
EGOV/FR/30.62	Categorization of the assets as per there nature (IT / Non-IT Asset).	
EGOV/FR/30.63	Mapping and tracking of asset (Fixed Assets, Damaged Assets and Assets to be returned)	
EGOV/FR/30.64	Provision for asset depreciation processing from time to time.	
EGOV/FR/30.65	Provision for sending the details to Finance for depreciation processing.	
EGOV/FR/30.66	Allocation of asset to particular user/group.	
EGOV/FR/30.67	Provision to raise requisition for a particular asset by an individual user / group.	
EGOV/FR/30.68	Provision to monitor the maintenance of the particular asset.	
EGOV/FR/30.69	Provision for request of asset location transfer in & transfer out.	
EGOV/FR/30.70	Auction for assets and base price.	
EGOV/FR/30.71	Receive payment (Online, Offline).	
EGOV/FR/30.72	Integration with Finance, Procurement, Sales, etc.	
31. Projects and Works Management		
EGOV/FR/31.1	Capital Investment Planning – To enable investment lifecycle management starting from short term / long term capital investment planning based on organization structure or any alternative structure that represents capital investment control organization, investment ideas, approval or rejection of investment ideas; allocation of funds for approved projects.	
EGOV/FR/31.2	Project: To enable project managers to better identify, select, prioritize, and manage projects. Including key performance metrics on budgets, schedules, and staffing. Solution to provide a centralised view of performance and at-risk elements. To also enable project managers to work closely together with team members and management. The comprehensive project management solution should enable RMC project managers to manage schedules, resources, assigned documents and materials, costs, and budgets. Team members need to be notified via workflow when they need to fulfil their project-related tasks thereby facilitating monitoring and control. Should have functionality to manage capital related work as well as operational expenditure.	
EGOV/FR/31.3	Scheduling Functions: To be able to schedule forwards and backwards according to the relationships between activities. Constraints need to be taken into account, with earliest and latest dates calculated, and floats determined. System should have integration facilities available for interfacing between third party products e.g. MS Project or Primavera.	
EGOV/FR/31.4	Document Management: Integration for drawings, technical specifications and other relevant project documents.	
EGOV/FR/31.5	Costs: The ability to plan costs using easy cost planning or by making use of the network calculation of internal and external work, services, and procurement planned in activities that are automatically calculated. The ability to map projects to internal orders or cost planning elements (WBS) elements to plan costs based on resource staffing and cost rates. Should have provision to maintain multiple versions of planned costs including base project cost plans, revisions in planned costs i.e. forecasting, calculation of estimated cost to complete. Should maintain a complete audit trail of changes carried out to any type of planned costs. Must have provision to provide necessary restriction to different users for carrying	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	out different activities related to planning of base costs and / or revision to original cost plans.	
EGOV/FR/31.6	Cost planning should have alternative options available from rough cut planning to detailed cost planning according to different stages of the project as the project progress.	
EGOV/FR/31.7	Budget the ability to control all expenditure during the execution phase. Additionally, the ability to break down the original budget into smaller packages of released budgets to allow an even more accurate availability control. System should have functionality to generate alerts based on pre-defined rule(s) in case of actual expenses or commitments exceed pre-defined limits.	
EGOV/FR/31.8	Resource and Time Management: The ability to assign resources and record time to resources assigned to any project or WBS- including for internal and external resources	
Project Execution		
EGOV/FR/31.9	The solution must enable the execution of a project based on the project plan including creation of documents, simulation of alternative project structures and analytics using Project system.	
EGOV/FR/31.10	RMC wishes to implement collaborative access to project documentation.	
EGOV/FR/31.11	Confirmation The solution must enable confirmation of actual time and costs for projects. The times entered become the actual times and costs for the project. Full change and cancellation handling are required. Approval of the time entered by appropriate authority should be available.	
EGOV/FR/31.12	Project-Oriented Procurement/ Repairs: Purchase Orders for goods and services will need to support multiple projects/WBS. Similarly, a single work order for repairs at the workshop may service multiple projects/WBS. System should have capability to identify goods procured for a specific project.	
EGOV/FR/31.13	Claim Management RMC and RSCL requires to track contract variations, change requests, e.g. scope, as well as handling claims and/or disputes, this will include costs and/or income. Should have functionality to manage the approvals for claims recorded.	
EGOV/FR/31.14	Project Cash Forecast During execution, need to integrate project cash management and provide accurate information on incoming and outgoing payments.	
EGOV/FR/31.15	Project Progress: analysis/earned value analysis will be needed to determine planned and actual project progress values. Need to provide information on the state of projects and how they are developing. Need to display milestone trend analysis with the relevant dates in a project at different report dates. This is required to analyse/forecast periodic statuses to include costs (e.g. actual, value of work done, forecast), income and outputs	
EGOV/FR/31.16	Progress Tracking: Required to closely monitor the progress of tasks and activities and monitor project specific purchase orders.	
EGOV/FR/31.17	Phase Approvals: Required to protect phase approvals by a structured approval process including decision makers named by RMC corporate policies and digitally signed approval documents. Workflow is required to support an efficient and effective process.	
EGOV/FR/31.18	Procurement Process must be able to access data from across RMC and RSCL departments and projects and consolidate the procurement process to provide a structured overview	
EGOV/FR/31.19	Project Reporting: Need a flexible, comprehensive information system to monitor and control project data. Need to evaluate individual projects, partial projects, or multiple projects. Include overview reports and reports offering various degrees of detail is designed to meet the needs of both project management and ordinary project personnel. RMC and RSCL wishes to analyse expenditure by asset types	
EGOV/FR/31.20	Project Structuring Required to create work breakdown structures (WBS) and networks, with their attendant activities and milestones. Structure a project using phases, tasks, checklists, and checklist items Integration may be required with external project scheduling package. System should have functionality to provide master project templates that can be used to create project structures especially for repetitive nature of projects.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/31.21	Project Costs: Required to plan costs using easy cost planning or by making use of the network calculation of internal and external work, services, and procurement planned in activities that are automatically calculable. Integration may be required with external project scheduling package.	
EGOV/FR/31.22	Budget Require budget availability controls for all project expenditure during the execution phase. Additionally, the original budget to be broken down into smaller packages of released budgets to allow accurate availability control.	
EGOV/FR/31.23	Scheduling Functions Requires scheduling capability of forwards and backwards task movements according to the relationships between activities. Constraints are taken into account, earliest and latest dates are calculated, and floats are determined. Additionally, require both bottom-up and top-down scheduling.	
Project Accounting		
EGOV/FR/31.24	Project Accounting: The solution must enable the precise planning, budgeting and monitoring of detailed activities costs of a project, both large scale such as building a treatment plant, and small scale projects. It is expected that Project accounting will fulfil different purposes in different phases of the project: - Help calculate the level of costs and the expected revenues when planning a project. - Once the costs have been approved, it will form the basis for allocating the budget. - During project execution, it must monitor and check variances in the costs. - Must meet the requirements of local accounting standards for construction related projects Must assist the project manager to ensure that the project is executed efficiently, on time, and within budget - which he or she achieves by ensuring that the required resources and funds are available as and when needed. RMC requires to report benefit achievements by project categories.	
EGOV/FR/31.25	RMC requirement to analyse work in progress by planned asset class to ensure prompt recovery of capital taxation allowances.	
EGOV/FR/31.26	RMC requires estimating, plan & capturing opex impact of capital investment.	
EGOV/FR/31.27	RMC may have some assets where value requires calculating/grossing up as provided by 3rd party.	
EGOV/FR/31.28	Integrated Planning and Tracking: RMC requires detailed financial integration including budgeting, cost planning and actual costs confirmations and commitments from various sources.	
EGOV/FR/31.29	Settle Financial Data: required to transfers costs to Financial Accounting, Asset Accounting and Management Accounting to establish cost of equipment for use in maintenance decisions regarding economic value of renewal.	
EGOV/FR/31.30	Development Collaboration requires to optimize a cross-enterprise asset/project development with internal and external teams including the sourcing of complex components. This requires a consistent central storage of all relevant data during the entire collaboration process and a secure integration of external partners and suppliers.	
EGOV/FR/31.31	Automatic generation of requisitions for procurement of materials and/or services required for a Project. The material/services should be made available to the project neither to too early nor too late	
EGOV/FR/31.32	Goods receipt of material and/or services specific to a project should load the costs on to the WBS. The material thus received should be reserved for the particular project and not be issued for other purposes	
EGOV/FR/31.33	Cost roll up : functionality should be made available to roll up costs from one WBS to another	
EGOV/FR/31.34	The module shall cover: - Classification of Works based on their types. - Maintain Vendor details - Maintaining rate schedules and revising the same - Defining a Project with Work Breakdown Structure - Estimation and submission for review and approval by the competent authority - Technical Sanction	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Administrative Approval as per the workflow defined - Integration with e-Tendering - Awarding Work Order to a vendor - Facility to track the project status by project code through portal. - Facility to input / upload data upon the measurement/progress of work done. - Provision to enter site inspection details/report in the system or upload site visit report - Completion Certificate - List of Projects - Projects-wise, location-wise reports etc. - Project status report.	
32. HR and Payroll System		
HR Management		
EGOV/FR/32.1	Talent Management: Require the ability to consolidate all the strategic employee development processes spanning the employees' career with the company from hire to retire, including recruitment, education, career development, and performance management. This should also encompass the company view of employee development, identifying and tracking high potential employees to ensure future leaders can be effectively promoted from within and that successors are identified for key positions.	
EGOV/FR/32.2	Employee Self Service: Requirement is to enable employees to do such as access their records to check personal information and update likes of addresses, contacts, next of kin, bank details in lines with best practice. To enable people managers to process authority to recruit, authority to appoint, changes to terms and conditions and with built in work flows to enable forwarding for authorisations and governance and ultimately flowing to personnel records update and generation of appropriate letters or contractual change conformations	
EGOV/FR/32.3	Manager Self Service: Requirement for people managers to process authority to recruit, authority to appoint, changes to terms and conditions and with built in work flows to enable forwarding for authorisations and governance and ultimately flowing to personnel records update and generation of appropriate letters or contractual change conformations	
EGOV/FR/32.4	Case Management: Requirement to track progress of Absence Disciplinary and Grievance Cases and monitor performance of Unit/Team or Individual and with the requirement to attach Microsoft Word or Scanned Handwritten letters to Case files.	
EGOV/FR/32.5	Performance Monitoring: Requirement to categorise transactional queries and escalate to Team Leader where SLA's are in "amber" or "red" status. Requirement to produce metrics relating to activity work load by Team and Individual.	
EGOV/FR/32.6	Integration required with the customer interaction portal, which would provide the source data for the transactional queries	
EGOV/FR/32.7	Requirement to capture details of contractors and consultants who might be paid through the procurement process via third parties.	
EGOV/FR/32.8	Workforce Analytics: Requirement the ability to produce metrics and Organisation charts relating to work force. Ability to do organisational modelling and workforce planning	
EGOV/FR/32.9	Employee Performance Management: Requirement to provide a flexible framework to integrate corporate goals and strategies with team and individual goals as well as integrate management-by-objectives. It should also provide functionality Requirement to be able to tie compensation to performance.	
EGOV/FR/32.10	Requirement to be able to capture individual development plans to roll up to training plans.	
EGOV/FR/32.11	Requirement to allow individual training courses and development steps to be displayed and monitored.	
EGOV/FR/32.12	Requirement to be able to produce metrics to show the distribution of individual performance within teams, departments, organization	
EGOV/FR/32.13	Require the ability for each employee to manage their career paths and aspirations, either through self-service capabilities or as a result of planning with their managers. This should include Requirement the ability to match profiles against	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	positions to determine skill and knowledge gaps which in turn are linked directly to training plans to fill the necessary qualifications. Require the ability to build structured career paths to give the employee guidance as to what the career progression might be based on their job within the organization.	
EGOV/FR/32.14	Compensation and Benefits Management Requirement: to operate Flexi Benefits including the ability to make payments to 3rd parties for provided benefits.	
EGOV/FR/32.15	Requirement to manage pensions administration as per RMC policies and rules	
EGOV/FR/32.16	Require the ability to streamline and integrate essential workforce processes such as employee administration, payroll, time management, absence recording, and legal reporting. This should enable the company to standardise and consolidate all workforce-related processes and data onto one platform, and ensure that adherence to local regulations and laws can be attained. Requirement to provide a central repository for employee data integrated fully with other business applications, especially maintenance and service delivery	
EGOV/FR/32.17	Requirement to "electronically" file documents including handwritten scanned letters to an employee personnel record. Requirement to produce individuals, teams and departments attendance / absence matrix and to "count down" sick pay entitlement, raise necessary alerts and correspondence are all requirements.	
EGOV/FR/32.18	Time and Attendance: Requirement to optimise processes for planning, managing, and evaluating the working times and activities of internal and external employees via the Time Management capabilities.	
EGOV/FR/32.19	Requirement to link RMC overtime rules to payroll to enable paperless/e-enabled automated authorisation and processing for payment to enable employees and managers to view attendees, holidays etc.	
EGOV/FR/32.20	HR Processes and Forms: The ability to automate paper-intensive and time-consuming employee-related processes such as hiring, termination, organisational reassignment, and maternity leave. Data entry and flexible workflow templates are required to enable the RMC to handle routine workforce processes quickly.	
EGOV/FR/32.21	To allow users to create project teams based on skills and availability, monitor progress on a project, track time, analyse results, and much more. The solution should empower users to eliminate redundant or ineffective projects, optimize productivity through the smarter use of resources, and manage the workforce as efficiently as possible.	
Payroll Management		
EGOV/FR/32.22	Ability to maintain leave records for computation of increments/pay revision with retrospective effect	

EGOV/FR/32.23	In addition to the standard payroll functions, the system should also comprise the following India-specific functions:
	- Indirect Evaluation
	- Basic Increments
	- Dearness Allowance
	- Housing
	- Car and Conveyance
	- Long Term Reimbursements
	- Fringe benefits
	- Income Tax
	- Third Party Deductions
	- Income from Other Sources
	- Tax on Arrears
	- Exemptions:
	  - Exemption on Leave Travel Allowance
	  - Exemption on Medical Reimbursements
	  - Exemption on Medical Insurance
	  - Exemption on Child Education Allowance
	  - Exemption on Child Hostel Allowance
	  - Exemption on Other Allowances and Reimbursements
	  - Exemption on Leave Encashment
	- Previous Employment Tax Details	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Professional Tax - Provident Fund - Employee State Insurance - Labour Welfare Fund - Nominations - Minimum Net Pay - Recovery of Rounding off Amounts - Loans Enhancement - One Day Salary Deduction - Mid-Year - Termination Work Bench - Gratuity - Superannuation Forms as applicable	
EGOV/FR/32.24	Ability to support configuration and parameterization of different pay components including facility to add/modify/delete pay components	
EGOV/FR/32.25	Ability to maintain employee data cost centre wise	
EGOV/FR/32.26	Ability to define pay structures at various levels and types (such as permanent, contract employees, consultants, trainees etc.)	
EGOV/FR/32.27	Ability to support calculation of different allowances based on user-defined criteria	
EGOV/FR/32.28	Ability to maintain all pay related rules (user definable) for automatic maintenance/ updating of data.	
EGOV/FR/32.29	Facility to indicate carryover and partial recovery	
EGOV/FR/32.30	Ability to generate monthly balance and cumulative balance position of various accounts related to payroll for user definable periods.	
EGOV/FR/32.31	Ability to support withholding of any amount recoverable from employee against salary, Gratuity and other dues payable to employee	
EGOV/FR/32.32	Ability to enter, administer and perform payroll for company loans, Voluntary Deductions, Recurring Payments/Deductions and additional payments	
EGOV/FR/32.33	Ability to prorate salary and allowance payment based on employee hire or resignation date	
EGOV/FR/32.34	The System must cater to: - Keep records of Sanctioned Posts - Employment in case of Death of any employee - Compassionate recruitment - Capture Employee Data – Employee Master - Employee Promotions - Transfer of staff - Leave Management - Enquiry, Punishment Process - Annual Confidentiality report Maintain Service Book	
EGOV/FR/32.35	Payroll Process: - Keep records of Sanctioned Posts - Employment in case of Death of any employee - Compassionate recruitment - Capture Employee Data – Employee Master - Employee Promotions - Transfer of staff - Leave Management - Enquiry, Punishment Process - Annual Confidentiality report Maintain Service Book	
EGOV/FR/32.36	Employee Self Service: - Keep records of Sanctioned Posts - Employment in case of Death of any employee - Compassionate recruitment - Capture Employee Data – Employee Master - Employee Promotions - Transfer of staff	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Leave Management - Enquiry, Punishment Process - Annual Confidentiality report Maintain Service Book	
EGOV/FR/32.37	Reports: - Attendance Register - Employee Detail Register - Transfer Detail report - Employee Pay Slip - Salary Summary Individual Report - Professional Tax Report - Pay Comparison Report - Bank Report - Yearly Salary Sheet Report - Income Tax Deducted Report - TDS Reports - Form 16 - Payroll register - Performance Report Appeals - Grievance Report (status, date of event and final ruling) - Workers compensation - Disciplinary actions (paid/unpaid etc.) - Future leave approval (e.g., approved, deferred, rejected) Leave status (vacation, sick, injury or any other user definable field)	
EGOV/FR/32.38	It should be noted that attendance information for employees may come from different sources. Hence integration will be required for field employees especially in the waste management system.	
EGOV/FR/32.39	Provision to manage the tour details of respective employee.	
EGOV/FR/32.40	Management of the service book records for each employee of RDA. – employee life cycle management	
EGOV/FR/32.41	Submission of CCR of subordinate RDA cadre staff to appropriate authority through the system	
EGOV/FR/32.42	Similarly submission of PAR by RDA cadre officer	
EGOV/FR/32.43	Provision for property declaration by individual employees in prescribed format.	
EGOV/FR/32.44	To keep information on suspension period/dismissal information along with charge frame, punishment etc.	
EGOV/FR/32.45	Keep information on assignment for enquiry, enquiry disposed/pending status	
EGOV/FR/32.46	Submission of TA bills through the system.	
EGOV/FR/32.47	Payroll: - Provision to employees where they can declare the savings and other expenses to ensure automatic reduction of tax deductions value. - MIS Reports on deductions like; LIC deposits, Bank Loans, CPF deposits etc. - Option to forward required salary data in specific format to OBC (Bank) through email for posting of gross salary to individual employee's accounts automatically. - Consolidated report on Annual salary particular including arrear drawn during the year for distribution among employees for facilitating income tax assessments. - All existing payroll data which is in dbase format (4th Pay, 5th Pay, 6th pay etc.) to be transferred to the new system so that, whenever required the arrear calculation and other reports of respective period can be generated. Option to be there for configuring the salary calculation as per 7th pay as well.	
33. Foundation Layer (Including Middleware, SOA,BPM, single sign on and integration with LDAP)		
EGOV/FR/33.1	The details of each layers/components & sub-components of system architecture are given below:	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/33.2	Access Channel: Integrated Portal services shall be accessed online through Web and Kiosks via several end user devices (PC, Tablets, Smart-phones, etc.).	
EGOV/FR/33.3	Single Sign On (SSO): System architecture should be SSO enabled: - Identity Provider: Active Directory Services (ADS) on MS-Windows Server 2012 R2 Standard Edition. - SSO Application: Web application that provides a secure SSO Application Interface including interface and secure web services for Identity and Application management lifecycle. - Process Flow: Only upon successfully authentication, the end-user shall land on the SSO Application wherein he would see a list of all the SSO-enabled applications. Once the authenticated user clicks on any application under the SSO Application, his/ her role/ access to that application is validated with Active Directory service in a secured manner and depending upon his role, access is denied/ granted to that application with the set of privileges mapped to the assigned role by that application. The user, after having finished his/ her work with the application, can go-back to SSO Application to select another application or directly Logout from the existing application. The SSO application would also enable an authenticated user to review/ update his profile (self-service) using the SSO application.	
EGOV/FR/33.4	Presentation Layer: The presentation layer i.e. User Interface shall be used for the receiving and delivery information for to and from the end-user of the application. It shall be responsive.	
EGOV/FR/33.5	Workflow Engine: Workflow shall be used with the automation of procedures where documents, information or tasks are passed among participants according to a defined set of rules to achieve, or contribute to an overall business goal. A workflow engine shall manage and monitor the state of activities in a workflow, such as the processing and approval of various application forms, and determines which new activity to transition to according to defined processes.	
EGOV/FR/33.6	ESB/Middleware: - An Enterprise Service Bus (ESB) is a software architecture model used for designing and implementing communication between mutually interacting software applications in a service oriented architecture (SOA). - The ESB supports SOAP Based integration, including SOAP/HTTP, SOAP/JMS, and SOAP/HTTPS and XML messages. - The ESB supports message record/ replay capability, many programming languages (Java, ESQL, PHP, C#, VB, F#, C++) including .Net, natively web services, Graphical Data mapping for transforming XML, text, and binary data, transaction management (Automatic, Commit, Rollback), SSL, SFTP, and LDAP etc. - The ESB provide robust transaction control capabilities including uncoordinated auxiliary transactions. - The ESB have the capability to support design, editing and manipulation of WSDL, through an integrated tooling. - The ESB provide an integrated testing tool with auto test the integration components developed and integrated development environment for development, test and deployment and debug. The ESB also support TLS 1.1 & TLS 1.2 to offer strict security requirements.	
EGOV/FR/33.7	Integration with other existing e-Governance applications and SCADA systems of Utility Companies for real-time monitoring, billing and support.	
EGOV/FR/33.8	Application Design, Development & Customization: - Compliance with industry standards: Solution shall be compliant with industry standards (their latest stable versions as on date) wherever applicable. This will apply to all the aspects of solution including but not limited to design, development, security, installation, and testing. - Platform Flexibility: Open Standards and Interoperability (Usage of standard APIs) shall be considered Web-centric, multi-tier architecture shall be used. - Iterative Development: Iterative approach shall be used to develop a software system iteratively and incrementally, allowing developers and users to take	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	advantage of lessons learnt during the development or earlier iterations of the system development. In the iterative development approach, the whole process of System Development typically iterates through all the phases of the System Development Life Cycle (SDLC), starting from gathering requirements to delivering functionality of a working release. - Compliance to SOA and EAI: Application shall be based on Service Oriented Architecture (SOA) and EAI. All modules of the application shall expose key functionality through Software APIs in form of SOAP & WS-* or JSON & REST etc. so that they can be consumed by other applications. User Interface: The application's UI should be based on HTML5 standard only and should be compatible with all devices like Desktop, Smartphone and tablet etc. The application interface should be responsive.	
EGOV/FR/33.9	Error Handling: Ensure applications execute proper error handling so that errors will not provide detailed system information, deny service, impair security mechanisms, or crash the system.	
EGOV/FR/33.10	Rich User experience: The solution shall have capability where any services like Payment Gateway, the mobile devices for queries/ reporting and providing day-to-day approvals by competent authorities as per authorized workflow for different kind of requests; and external entities like bank, departments and others can invoke this framework by passing the required parameters and specifying the desired output.	
Technology Standards		
EGOV/FR/33.11	Browser Compatibility: The Integrated Application shall support common web and mobile browsers like Google Chrome, Internet Explorer, Firefox, Safari and Opera Mini etc.	
EGOV/FR/33.12	Multi-Lingual Support: Application shall support at least Unicode 5.1/ 6.0 standard based Tri-lingual versions for user interface. It is expected to be in the Oriya, Hindi and English (India) languages.	
EGOV/FR/33.13	Anywhere Access: Application shall be deployed on state government cloud to enable anytime, anywhere access and to address auto sync/ save, efficiency, peak load handling issues. Application shall be accessible on all popular devices (PC, mobile or tablets) and across all popular operating system platforms like Windows/ Apple for PCs and Android/ IOS for mobiles. The Integrated e-Office application should also function on the low bandwidth (64 Kbps/ GPRS).	
EGOV/FR/33.14	Scalability, Reliability and Flexibility: The technology shall be scalable with Department's emerging requirements and information handling needs of the government. The architecture must be scalable and flexible for modular expansion. The IA shall plan and provide for horizontal scalability in such a manner that a new server can be added (or removed) dynamically, as and when required in future, without disturbing the normal functioning of production system. The vertical scalability in servers in terms of additional processors and RAM will have to be provided for handling future growth in transactions.	
EGOV/FR/33.15	Interoperability: The system shall be interoperable and should comply with open standards for easy integration. The entire system/ subsystem should be interoperable, in order to support information flow and integration. Operating systems and storage technologies from several suppliers must interact well with each other.	
Security Standards		
EGOV/FR/33.16	Application Access: Ensure applications processing data properly for authenticated users (through central authentication systems), specifically: SSO Login. Establish authorizations for applications by affiliation, membership, or employment, rather than by individual. If individual authorizations are used, these should expire and require renewal on a periodic (at least annually) basis.	
EGOV/FR/33.17	Review: Conduct code-level security reviews with professionally trained peers for all new or significantly modified applications; particularly, those that affect the collection, use, and/or display of confidential data. Conduct annual security tests of Internet applications.	
EGOV/FR/33.18	Security: application shall support both HTTP and HTTPS (SSL certificate shall be provided).	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
34. Enterprise Content Management (ECM) System / Document Management System		
EGOV/FR/34.1	Facility to scan and upload – Paper documents – Photos – Email communication Any other document;	
EGOV/FR/34.2	Documents in electronic soft form (pdf, txt, xls, doc, ppt, picture files, TIFF, JPEG, GIF, even Zip Files) System generated documents	
EGOV/FR/34.3	Ability to share documents scanned across several offices / departments.	
EGOV/FR/34.4	The proposed system shall have Out of the Box capability of Digital Asset management to manage rich media content files.	
EGOV/FR/34.5	Automatically create multiple formats of a corporate image or video and create additional formats with various aspect ratio on ingestion	
EGOV/FR/34.6	Support multiple definitions of sets of renditions to be created for different classes of assets	
EGOV/FR/34.7	System shall have support for management of image formats such as JPG, GIF, PNG, TIFF, PSD, and BMP; as well as output formats such as JPG, GIF, PNG, and PSD.	
EGOV/FR/34.8	System shall have support for video formats such as Flash, Real, Windows Media Format, QuickTime, and others. Image and Video metadata is extracted and associated with the content item as object metadata.	
EGOV/FR/34.9	Ability to check the quality of the scanned image and make corrections/adjustments to improve the quality of the scanned image.	
EGOV/FR/34.10	The ECM shall support temporarily storing the scanned images locally before uploading to the central server.	
EGOV/FR/34.11	Ability to support quick scanning and indexing of bulk documents. Scanning through browser plug-in.	
EGOV/FR/34.12	Ability to support automatic cropping / masking of whole/any part of the document. This ability should be user defined and also document wise.	
EGOV/FR/34.13	It shall be possible to scan and upload documents including pictures and images. Such document may be uploaded directly from third party premises over the web or from the office.	
EGOV/FR/34.14	Ability to support Web based scanning	
EGOV/FR/34.15	It shall be possible to set up and track both mandatory and non-mandatory documents.	
EGOV/FR/34.16	Document types need to be pre-defined as a product / type of service / transaction type / workflow etc.	
EGOV/FR/34.17	Confirm that the content was delivered and viewed as a proof of compliance with security policies	
EGOV/FR/34.18	Grant access to documents offline for a specified period of time while maintaining audit capabilities.	
EGOV/FR/34.19	The system shall have a native iOS and Android based mobile/tablet app for easy access of the information (document) while users are on the move.	
EGOV/FR/34.20	Workflow for routing and tracking of documents, messages and Forms	
EGOV/FR/34.21	Create Ad-hoc or predefined routes for automatic document routing on sequential / parallel routes. This must be offered as a base and standard product	
EGOV/FR/34.22	Facility of associating a note-sheet with the file enabling users to comment and review.	
EGOV/FR/34.23	Facility of attaching documents and folders in work items	
EGOV/FR/34.24	Facility to act upon, forward, return or complete Work-items	
EGOV/FR/34.25	Support for referring Work-items to other users outside the pre-defined route	
EGOV/FR/34.26	Time –based/ Event -based reminders	
EGOV/FR/34.27	Provision of putting shared and secured notes for collaborative working on Work items	
EGOV/FR/34.28	Ability to support typical document imaging annotations which include:	
EGOV/FR/34.29	Highlighting images and text in various colours to emphasize words or sections	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/34.30	Redacting (blacking-out or whiting-out) images and text to preserve confidentiality	
EGOV/FR/34.31	Stamping images with words such as FAXED or CONFIDENTIAL, or with signatures denoting approval or denial	
EGOV/FR/34.32	Attaching sticky notes that contain additional comments	
EGOV/FR/34.33	An imaging system 's security should control who can view	
EGOV/FR/34.34	Annotations such as highlighting, stamps or sticky notes, and who can see through redaction. All annotations should be overlaid and not change the actual image.	
EGOV/FR/34.35	Ability to support Printing, faxing and e-mailing documents	
EGOV/FR/34.36	System shall provide web-based administration tool and provide a single point of access for managing and administering all repositories, servers, users and groups regardless of their location across the enterprise	
EGOV/FR/34.37	The system shall allow content syndication service via xml based feeds , email alerts etc.	
EGOV/FR/34.38	The system shall support versioning of contents, user should be able to access previous and next versions	
EGOV/FR/34.39	Shall support storage of complete and multiple versions of content	
EGOV/FR/34.40	Shall have major & minor release for draft & final release version of the document	
EGOV/FR/34.41	Shall support the JSR 170, Java APIs/REST APIs/Web Service APIs that make content assets available to the application layer services or other Content Management (CM) solutions.	
EGOV/FR/34.42	Shall support for storage of any type of contents such as JPG, TIFF, PDF, MS office files, audio, video, auto cad files etc.	
EGOV/FR/34.43	The product shall support single metadata store for modules such as Document Management, Web Content Management, Records Management and Digital Asset Management	
EGOV/FR/34.44	System should provide library services such as core content services, workflows, archiving, folders, content publishing, records management and security features.	
EGOV/FR/34.45	Ability to support a single Security model for the content repository that is used to manage documents, records as well as web content.	
EGOV/FR/34.46	Shall have out of box support for standards like BPM/BPEL to address complex workflow requirements.	
EGOV/FR/34.47	System shall support for auditing for usage of content through audit trails.	
EGOV/FR/34.48	System shall provide support for scheduling indexing.	
EGOV/FR/34.49	Provides ability for administrators to archive and backup content.	
EGOV/FR/34.50	Shall support for both centralized & distributed architecture.	
EGOV/FR/34.51	Shall support for content cache for remote client.	
EGOV/FR/34.52	Shall have policy-based, pluggable framework for reliability and secure access.	
EGOV/FR/34.53	Shall have a comprehensive access control functions, depending on the user role & access levels	
EGOV/FR/34.54	Shall support simple as well as complex workflows along with escalation routing and monitoring policy as defined by user	
EGOV/FR/34.55	The proposed system shall be able to classify any piece of content as a record	
EGOV/FR/34.56	Support for creation, declaration, classification, retention and destruction of business records.	
EGOV/FR/34.57	System shall provide audit trails and certificate of destruction.	
EGOV/FR/34.58	System shall provide the ability to freeze the records.	
EGOV/FR/34.59	Product shall provide records managers with a single view into all retention schedules, disposition actions, and audit histories, facilitating the process of identifying and declaring records.	
EGOV/FR/34.60	System shall allow for management of external content.	
EGOV/FR/34.61	System shall support adapters to external repositories for managing records, such as file systems, content repositories and e-mail archives	
EGOV/FR/34.62	Product shall provide generic adapters that can be configured for integration with other applications and repositories.	
EGOV/FR/34.63	It shall have out of box components and integration options with Portal	
EGOV/FR/34.64	The system shall provide ability to leverage multiple display templates for a content item	
EGOV/FR/34.65	System shall support in-context web content contribution, preview, updates and	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	approvals.	
EGOV/FR/34.66	System shall provide support for multi-site management	
EGOV/FR/34.67	The system shall provide spell-checking functionality. The language of the dictionary must be able to be changed for content authors producing content in other languages.	
EGOV/FR/34.68	The system shall provide the ability to upload and associate media items to content items from within the content item authoring interface.	
EGOV/FR/34.69	The system shall provide the ability to preview content as it will appear on pages where it is added in production prior to it being published	
EGOV/FR/34.70	DAK and File Management system should comply with the Manual of Office Procedure (MOP), published by the Department of Administrative Reforms and Public Grievances (DARPG).	
EGOV/FR/34.71	The system should have an Interface for uploading the scanned copies of documents / letters.	
EGOV/FR/34.72	The system shall provide an integrated scanning engine with capability for centralized and decentralized Scanning & Document Capturing. The scanning solution should directly upload DAKs/Correspondences in Document management system/File Management System.	
EGOV/FR/34.73	The system shall provide facility to view all letters/documents at the right hand side (RHS) with note-sheet on left hand side (LHS). The system should have mobile app for Dak and file capture.	
EGOV/FR/34.74	Scanning - Both bulk and web scan capabilities, Automatic extraction of data using OCR, Automatic file and document separation using blank separator, barcode separator and fix, Automatic correction of parameters like improper resolution, format/ compression not proper, skew, wrong orientation, error in automatic cropping, punch hole marks etc. during scanning	
EGOV/FR/34.75	The system shall provide an advanced search interface for tracing & searching a correspondence (DAKs) based on dates, subject, pending with, completed by, pending since etc.	
EGOV/FR/34.76	The system shall provide facility to users to append their notes, which shall be automatically stamped with user name, date and time	
EGOV/FR/34.77	The system shall have an In-built Web based Text Editor with basic functionalities such as bold, alignment, font, color etc. for writing the notes.	
EGOV/FR/34.78	File/DAK Management System should be based on Manual of office Procedure (MOP from DARPG- Department of Administrative Reforms And Public Grievances)	
EGOV/FR/34.79	Module should include DAK/File Management with features like online DAK/File register etc.	
EGOV/FR/34.80	Module should support Green Note sheet	
EGOV/FR/34.81	The Document Management System would have a simplified and standardized way to access the documents, using an Industry standard and best of the breed solution complying to industry level open standards for Document Management System.	
EGOV/FR/34.82	The Office Note module should have features such as an In-built Web based Text Editor with basic functionalities such as bold, alignment, font, color etc. and a draft folder to save Office Notes that are created through in-built text editor, The ability to route the Office Note for approval, Search and check the status of a Note in workflow, Facility to add the approved Office Note in a File.	
EGOV/FR/34.83	Creation of new file and attaching any letters to it.	
EGOV/FR/34.84	Generation of unique number for the respective file.	
EGOV/FR/34.85	Defining user privilege for accessing any file.	
EGOV/FR/34.86	Provisions to limit the access of the file / document which will help maintain its security.	
EGOV/FR/34.87	Provision to send file to respective user / group.	
EGOV/FR/34.88	Tracking and monitoring of files.	
EGOV/FR/34.89	Meta-tagging of the files for easier search.	
EGOV/FR/34.90	Mechanism for effective and efficient search for all the old records.	
EGOV/FR/34.91	Appropriate storage structure for the files.	
EGOV/FR/34.92	Provision for marking files as; Urgent, Most Urgent etc.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
EGOV/FR/34.93	Similarly files put up for RTI, Grievance, Court matters to be highlighted accordingly.	
EGOV/FR/34.94	Provision for giving notes through the system.	
EGOV/FR/34.95	Employee-wise MIS report on total number of files generated, number of files disposed or pending during specific period, which may be helpful for proper distribution of work.	
EGOV/FR/34.96	Reports on average days taken for disposal of files, un-disposed files pending since average no. of days which may present performance of the employee.	
EGOV/FR/34.97	Alerting the employee on marking of new files by blinking indicator on screen as well as through SMS only for Urgent & Most Urgent marked files.	
EGOV/FR/34.98	Alerting the employee time to time for non-disposal of files within permitted time limit.	
EGOV/FR/34.99	Integration with existing Document Management System software."FineDOC" under which number of old files are scanned & stored.	
EGOV/FR/34.100	Digital Certificate Services The system should automatically enable/disable the Digital Signature Certificates (DSCs) of employees depending on the current status of each employee namely, fresh appointment / transfer / leave/ training / retirement etc. The system should accordingly enable DSC only for an "active" employee. Procurement of digital certificates for the users of the RMC will be the responsibility of the client.	
EGOV/FR/34.101	MAILING AND MESSAGING SERVICES This would be used for sending the alerts as mail and SMS message to the registered users of the application and will be used for messaging and calendaring services. The Mail and SMS Server should provide a highly available, scalable and reliable platform for delivering secure communication services. It would be required to cluster this Server to ensure high availability and reliability. This server will also act as Messaging Server. It should provide with extensive security features ensuring the privacy of users and the integrity of communication through user authentication, session encryption, and content filtering to help prevent spam and viruses, and mechanisms to monitor and enable regulatory compliance. It should support standard SMTP, IMAP and POP3 services. The Messaging system should provide a secure messaging and collaboration – email solution with standard features like calendaring, contacts and tasks, Archiving, Directory and LDAP address book, web based access to emails and support for data storage. Other features to be supported include – per-user filtering policies, user management, mailing list manager and synchronization with MS Outlook / Lotus Notes/equivalent. Approximate size of mailbox for registered user should be 300MB.	
EGOV/FR/34.102	PAYMENT GATEWAY The application would provide the online payment services through integration with the payment gateways. The solution shall support card payments using all the popular debit and credit cards (Visa, Master card etc.) and Direct Debit. For online payments, Secure Socket Layer (SSL) shall be used for supporting & securing the transactions taking place through the payment gateway. As Commercial transaction over internet is prone to Identity Theft and can cause financial loss to department and citizens, the solution would incorporate PCI DSS ver. 1.1 standards.	
35. Integration and Interfaces		
EGOV/FR/35.1	The RMC functionality requirement is to create a SOA based enterprise framework to enable online integration for the various components as per the solution proposed by the MSI. This framework must include: - E Governance System - Command and Control System - Document Management System - Portal - Multi-channel communication interfaces which includes devices like desktops, laptops, tablets, mobile/handheld devices working on Android, Apple ,Windows or any other contemporary platform - Emails and SMS services - Web GIS - SCADA systems	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	- Payment Systems (not limited to RTGS, PAYTM, BHIM, Credit Cards etc.) - Banks - Waste Management System - Fleet Management Systems and Vehicle Tracking Systems - Traffic Management Systems - Systems relating to central and/ or state governments - Websites/portals of central and/or state governments - Systems owned by Vendors and/or City Operators - Police, Fire Brigade and other relevant state agencies - Systems/portal relating to any other domestic or international organisation as per RSCL business needs Any other system to be included in the proposed solution by the MSI	
EGOV/FR/35.2	Functionality should be provided for validation of data movement between source and target system	
EGOV/FR/35.3	Functionality should be provided to prevent duplicate updates of batch data files provided by external entities. The scope of this requirement should not be limited to the following illustrative example like reconciliation statements provided by Banks	
EGOV/FR/35.4	Not with standing anything contained in this RFP, the MSI solution cover all RMC business needs and should specify if the required interfaces needs to be bi-directional or uni-directional. During the course of the implementation there could be a RMC business needs which may arise which should be included in the MSI scope of work.	
EGOV/FR/35.5	The RMC requirement is for online integration as a default. The MSI should propose a batch interface only because it is justified by business exigencies	
36. Integration Requirements for all modules		
EGOV/FR/36.1	Document/workflow Management System	
EGOV/FR/36.2	Mailing and Messaging System	
EGOV/FR/36.3	SMS Gateway	
EGOV/FR/36.4	Accounting System	
EGOV/FR/36.5	Finance System	
EGOV/FR/36.6	Payment Gateway	

Citizen Facilitation Center

S. No.	Minimum Functional Requirement	Compliant (Yes / No)
Employees Assistance		
CFC/FR/1.1	The citizen facilitation centre would be manned by trained employees of the city. - Employees shall assist the citizens with information, application or complaints. - Employees shall also take care of e-mail, postal service letters and phone calls. - Employees shall log into the portal and conduct the business required for the citizen.	
Citizen Helpdesk		
CFC/FR/2.1	• Facility to lodge New Complaints, Check Status - Integration Required with Grievance Redressal Module	•
CFC/FR/2.2	• Facility to check citizen data - Birth / Death registrations - Bill Dues - Application Status - Payment Status - Renewal Status - Integration required with all Modules.	•
CFC/FR/2.3	• Facility for Citizen Charter - Integration Required with Grievance Redressal Module	•

S. No.	Minimum Functional Requirement	Compliant (Yes / No)
Application Acceptance & Delivery Outputs		
CFC/FR/3.1	Department-wise categorization	
CFC/FR/3.2	Allow system to accept service specific inputs	
CFC/FR/3.3	Capture of Mobile No. & E-Mail of Applicant	
CFC/FR/3.4	Re-submission of rejected application after compliance	
CFC/FR/3.5	Check-list for documents to be submitted along-with Application	
CFC/FR/3.6	Define citizen charter (list of the officers & duration for service delivery)	
CFC/FR/3.7	Fees to be accepted - Integration required with accounts	
CFC/FR/3.8	Generate Token of Application acceptance	
CFC/FR/3.9	Rejection Note in case of inadequate application	
CFC/FR/3.10	Marking the application to Corresponding department /Ward / Officer - Integration Required with Workflow Module	
CFC/FR/3.11	Delivery of the output through CFC or Internet - Integration Required with Departmental Modules	
CFC/FR/3.12	Payment Acceptance - Integration Required with Accounts and Departmental Modules - Property Tax - Water Bills and Power Bills - License - All Departmental Services - Tender Document Fees - Any Other	
CFC/FR/3.13	Citizen Services (General) - Integration Required with Accounts and Departmental Modules - Nursing Home Registration (as applicable) - Registration of Hospitals - NOCs for other govt. departments - Tree Cutting / Trimming Service - Road / Water / Drainage / Electrical - Any Other Service	
MIS		
CFC/FR/4.1	SMS alert to applicant upon decision	
CFC/FR/4.2	- Services Statistics - CFC-wise - Department-wise	-
CFC/FR/4.3	Officer-wise list of services pending beyond the stipulated time - Integration Required with HRMS	

Integrated Multi-Services Digital Kiosks

S.No.	Minimum Functional Requirement	Compliant (Yes / No)
IDK/FR/1.1	Integrated Multi Services Digital Kiosks shall have integrated: - Emergency Call Button (ECB) - PTZ CCTV - Wi-Fi access point - Ability to pay bills using e-wallet, debit card and credit card. - Touch Screen for availing citizen services with in-built interactive platform - Integration with environmental sensors to display information from various sensors - Solar Panel with batteries	

S.No.	Minimum Functional Requirement	Compliant (Yes / No)
	- Charging Slots - Static Advertisement around three faces - Microphone - Speaker - Keypad for entry of PIN for authentication - Printing of any receipts - All these components shall be supplied as part of the integrated multi services digital kiosk	
IDK/FR/1.2	Integrated Multi-Services Digital Kiosk's power requirements shall be met with support of raw power for backup purposes.	
IDK/FR/1.3	Integrated Multi-Services Digital Kiosk shall be fixed units, embedded inside the ground that shall be weatherproof.	
IDK/FR/1.4	Integrated Multi-Services Digital Kiosk enclosure shall have the space to house all the hardware equipment required for the Multi-Services Digital Kiosk including switches, solar panel, batteries, printer for receipts and other associated accessories. All the wiring shall be concealed within the Multi-Services Digital Kiosk enclosure and shall not be visible from outside.	
IDK/FR/1.5	The Emergency Call Button (ECB) shall have the capability to trigger emergency communications with ICCC. As the Emergency Call Button is pressed, the call should land up to the operator at the ICCC from where it may be routed to the concerned department.	
IDK/FR/1.6	The ICCC operator shall able to monitor the video of the user who triggered the ECB. Automatic video recording shall be enabled when ECB button is pressed at multi-services digital kiosks.	
IDK/FR/1.7	Integrated Multi-Services Digital Kiosk shall have in-built speakers and microphone for making an emergency call to/from the ICCC and a keypad for accepting user input.	
IDK/FR/1.8	The integrated PTZ CCTV shall have the capability of recognition. Operator at the ICCC shall be able to monitor the live feed from the CCTV. When the emergency button is pressed, the PTZ camera shall automatically focus on the person using the button with a video feed at the video wall at the ICCC.	
IDK/FR/1.9	The Integrated Multi-Services Digital Kiosk shall have in-built charging slots i.e. two (2) USB ports and one (1) three pin standard plug port.	
IDK/FR/1.10	The user-interface panel shall built-in capacitive touch screen for interactive purposes including but not limited to: - Maps and navigation services i.e. displaying routes across Rourkela - Displaying of bus routes across Rourkela - Information about Rourkela along with e- governance services. - Environmental related information via integration with environmental sensors. - Places of attraction in Rourkela - Places near me services which may include hotels, government offices, shops, tourist attraction, etc. - Information about the events. - Emergency contact numbers such as hospitals, police, fire, etc. - Integration with e-governance system. - Integration with digital wallets, credit and debit cards for payments.	
IDK/FR/1.11	Integrated Multi-Services Digital Kiosk shall have capabilities for making digital payments for: - Utility Bills for government services such as electricity, water, Wi-Fi, etc. - Citizen services - Tickets for the events around the city - Any other RSCL/RMC supported activity/event	
IDK/FR/1.12	Integrated Multi-Services Digital Kiosk shall have in-built receipt/ticket printer having the functionality of printing of receipts, any other tickets, etc.	
IDK/FR/1.13	The Integrated Multi-Services Digital Kiosk shall have the space for providing the static advertisement around three (3) faces.	

S.No.	Minimum Functional Requirement	Compliant (Yes / No)
IDK/FR/1.14	The Integrated Multi-Services Digital Kiosk shall be multilingual i.e. it shall support languages such as English, Hindi and Oriya.	
IDK/FR/1.15	The Integrated Multi-Services Digital Kiosk shall have ECB and touch panel at an average height of 1.5m above ground.	
IDK/FR/1.16	Integrated Multi-Services Digital Kiosk shall be upgradable through a central system remotely over internet.	
IDK/FR/1.17	It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network.	

Standalone Multi-Services Digital Kiosks

S.No.	Minimum Functional Requirement	Compliant (Yes / No)
Standalone Multi-Services Digital Kiosks		
SDK/FR/1.1	Stand-alone Multi Services Digital Kiosks shall have integrated: - Ability to pay bills using e-wallet, debit card and credit card. - Touch Screen for availing citizen services with in-built interactive platform - Integration with environmental sensors to display information from various sensors - Keypad for entry of PIN for authentication - Printing All these components shall be supplied as part of the stand-alone multi-services digital kiosks.	
SDK/FR/1.2	Stand-alone Multi-Services Digital Kiosk enclosure shall have the space to house all the hardware equipment required for the Multi-Services Digital Kiosk including switches (if applicable), printer for receipts and other associated accessories. All the wiring shall be concealed within the Multi- Services Digital Kiosk enclosure and shall not be visible from outside.	
SDK/FR/1.3	The user-interface panel shall built-in capacitive touch screen for interactive purposes including but not limited to: - Information about Rourkela along with e- governance services. - Maps and navigation services i.e. displaying routes across Rourkela. - Displaying of bus routes across Rourkela - Places of attraction in Rourkela. - Places near me services which may include hotels, government offices, shops, tourist attraction, etc. - Information about the events - Emergency contact numbers such as hospitals, police, fire, etc. - Integration with e-governance system. - Integration with digital wallets, credit and debit cards for payments.	
SDK/FR/1.4	Stand-alone Multi-Services Digital Kiosk shall have capabilities for making digital payments for: - Utility Bills for government services such as electricity, water, Wi-Fi, etc. - Citizen services - Tickets for the events around the city - Any other RSCL/RMC supported activity/event	
SDK/FR/1.5	Stand-alone Multi-Services Digital Kiosk shall have in-built receipt/ticket printer having the functionality of printing of receipts, any other tickets, bus tickets etc.	
SDK/FR/1.6	The Stand-alone Multi-Services Digital Kiosk shall be multilingual i.e. it shall support languages such as English, Hindi and Oriya.	
SDK/FR/1.7	Stand-alone Multi-Services Digital Kiosk shall be upgradable through a central system remotely over internet.	
SDK/FR/1.8	It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network.	

Mobile App

S. No	Minimum Functional Requirements	Compliant (Yes / No)
Informative Services		
SCA/FR/1.1	About Rourkela" shall provide details about Rourkela city in GIS platform and shall comprise, history of Rourkela, accessibility information, climate, local cuisines, important festivals, key business locations, places of interest including heritage spots, weekend getaways, nature discovery, farm tourism, facts at a glance, accommodation and dining options, gallery (Photos & videos), etc. Some of these are detailed below: - "Facts at a Glance" giving details about area, population, currency, religion, linking roads, postal code, longitude, latitude, area, altitude, population, literacy rate, STD code, average rainfall, villages, language and best season to visit - "Health Centers" giving details of Govt. and Private Hospitals, Blood Banks, Ambulances, Medicals and Diagnostics centers - "Education Hub" giving details of Universities, Colleges, Schools, Gymnasiums and Sports club, Teaching Institutes, Study Centers and Libraries along with navigation route - "Toilets" giving location of nearest Public/Community Toilet - "Recreation Centers" giving location of Parks, Gardens, Temples, Auditoriums, Sports Stadium, Community Centers, Theatres, Multiplexes, Trekking and Adventure Parks - "Tourist Spots" giving details of tourists spots within or near the city, Shopping Spots, and Souvenirs, museums, recreation centers, etc. - "Dining" Section with detailed listings of various restaurants including those in geographical proximity using google map functionality (i.e. Restaurants around Me). Also show Travel Distance (length of time in minutes and km or miles) via walking, driving to the listings - "Reviews & Ratings" can be attached with each location so as to give the user a basic idea of the landmark - "Events and Entertainment" with a focus on what is happening and available that evening. May include the ability to add to user's calendar - "Air Quality" giving details of weather conditions of the city for the current day along with five past days conditions and next five days future predictions. - "Know Your Ward" giving details of ward-wise number of households, number of slums, population of ward, list of schools, list of colleges, list of hospitals, ongoing and planned development activities	
SCA/FR/1.2	Alerts related to emergencies, Government notifications and campaigns, weather information (for fishermen and farmers), tax reminders, pensions, etc.	
SCA/FR/1.3	Alerts to nearest hospitals and police stations during accidents/ disasters	
SCA/FR/1.4	Reporting suspicious activity to Law Enforcement agencies	
SCA/FR/1.5	Employment opportunities (job ads, availability of jobs under NREGA)	
SCA/FR/1.6	Contact information for all the places listed in the app shall be regularly updated and the app shall have the feature to instantaneously dial the contact numbers through one press of the call icon	
Transactional Services		
SCA/FR/2.1	Holding Tax, Trade License, Electricity Bill, Water Bill, Birth Certificate, Register a Birth/Death, booking of cesspool vehicles, etc.	
SCA/FR/2.2	No-Dues/No-Objection certificate issued from Rourkela Municipal Corporation (RMC)/Rourkela Development Authority (RDA)	
SCA/FR/2.3	Online ticketing/ entry passes (QR based) for entry to heritage/tourist sites	
SCA/FR/2.4	RTI filing, applying for government services, license renewals, etc.	
Interactive Services		
SCA/FR/3.1	Generation of unique customer identification number for every grievance	
SCA/FR/3.2	Categorization of Grievance regarding various services provided by city administration including pot holes, street light maintenance, encroachment issues, sanitation/public health, septic tank/containment unit cleaning related etc. including facility to upload geo-location tagged pictures.	
SCA/FR/3.3	Acknowledgements and status updates related to delivery of public services	

S. No	Minimum Functional Requirements	Compliant (Yes / No)
SCA/FR/3.4	General and service specific feedback	
SCA/FR/3.5	Ability for users to share their comments with friends and networks via Facebook, Twitter YouTube channel & Google Plus	
SCA/FR/3.6	Ability for users to rate the App and to add / surf comments	
SCA/FR/3.7	Push notifications to users with ability for the user to Accept / Decline receiving these notifications; Turn notifications On / Off	
SCA/FR/3.8	Enable RMC to solicit citizen responses on various topics through polls/ surveys.	
SCA/FR/3.9	Platform shall enable RMC to seek participation from city residents for various activities and help them volunteer for events, causes etc.	
SCA/FR/3.10	Uniform/ single pre-designated numbers (long and short codes) shall be used for mobile-based services to ensure convenience: e.g. 51969 and 166 procured by DeitY for M-Gov Services	
Safety Services		
SCA/FR/4.1	Stores five emergency contact of choice	
SCA/FR/4.2	Sharing of current location with Pre-Stored Emergency Message via SMS indicating the Latitude and Longitude of current location with the Link to open the location in Google Maps to the stored 5 emergency contacts in a single click/shaking phone	
SCA/FR/4.3	Call option to Police, Ambulance and Fire service	
Integration with external applications		
SCA/FR/5.1	City Bus Tracking, Air Quality Monitoring System, GIS for Direction and Maps - For informative services, the application must be integrated with specified aspects to provide the needed relevant information related to it to the residents and tourists	
SCA/FR/5.2	Web Portal of RSCL/RMC/RDA, WESCO and PHEO - For transactional and interactive services, the application must be integrated with specified organization to enable residents to pay for various city vide services as well as register their grievances	
SCA/FR/5.3	Police, Fire and Ambulance - For safety services, the application must be integrated with specified facilities to enable them to the SOS site	
SCA/FR/5.4	SMS/Mail - To facilitate the services of the application and provide the needed status updates to the user the application must be integrated with SMS/Mail system	
Content Management System		
SCA/FR/6.1	CMS shall support login module using which content authors will be able to login	
SCA/FR/6.2	CMS shall contain a WYSIWYG editor and provide standard Word authoring features (also known as a Rich Text Editor) to enable an editor to add and format text, links, and images to content areas, create tabular layouts within a text area and apply styles	
SCA/FR/6.3	CMS shall support drag and drop feature to enable easy management of content. The CMS shall support the following minimum preview and publication functions: • Preview only on CMS (not visible to users) • Save as unpublished (draft) • Preview on Portal • Unpublish (save as unpublished, not visible to users) • Publication scheduling • Publication expiration date (automatic unpublish)	
SCA/FR/6.4	CMS shall contain content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e. before becoming visible to the public)	
SCA/FR/6.5	CMS shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e. define the targets within the workflow)	
SCA/FR/6.6	Layout and content shall be managed separately (i.e. it must be possible to create and edit content without having to amend or create a template)	
SCA/FR/6.7	CMS shall support the creation and application of styles using Cascading Style Sheets (CSS) enabling the swift alteration of the look and feel (color, font, image size and positioning, link attributes, table properties)	
SCA/FR/6.8	CMS shall offer the ease-of-use features like Friendly URL's, Spell Checker, Undo etc.	
SCA/FR/6.9	CMS shall include a social media integration module that allows configurable publishing of content (pages, interactive data visualizations, images, videos) to a variety of social media (Facebook, Twitter, Google+, LinkedIn, Pinterest, Tumblr, etc.)	
SCA/FR/6.10	CMS shall support creation of templates and styles reflecting Rourkela Smart City	
SCA/FR/6.11	Limited CMS shall support version control (check-in, check-out, number of versions)	

S. No	Minimum Functional Requirements	Compliant (Yes / No)
	and it must be possible to restore previous versions of a content item branding	
SCA/FR/6.12	The CMS shall provide reports for following: • Audit Log Screen will be provided to admin user to check the activities performed by all users. The data will be available only in read-only mode. • Admin User will be able to see the list of login/logout information for the user through Authentication report screen. • Admin User will be able to see the list of notifications sent to the devices through notification screens. Data will be only in read only mode. • Google store, Apple store, etc. dashboard details regarding total downloads, crashes, uninstalls, etc.	
Application Management		
User Registration		
SCA/FR/7.1	It shall enable user to register themselves	
SCA/FR/7.2	It shall highlight the mandatory fields to be filled for registration	
SCA/FR/7.3	It shall also have optional fields to be filled with regard to consumer/other identification numbers to make payment for city services	
SCA/FR/7.4	It shall support mobile authentication with OTP for registration	
SCA/FR/7.5	It shall also support mass registration through file upload for admin users	
SCA/FR/7.6	Interests to be captured at the time of registration and relevant events push notifications to be sent to users via email, SMS and Mobile Push Notifications	
SCA/FR/7.7	Module shall have the facility to accept social media logins such as Facebook, Twitter, and Google Plus, etc.	
User Login		
SCA/FR/7.8	Registered users using their credentials shall be able to login to the application and then shall get redirected to the home page	
SCA/FR/7.9	Login module shall have forgot password mechanism. In case user forgets the password/wish to reset password, a link shall be sent to user's registered Email address or by sending OTP on registered mobile to reset password	
Administration of users and groups		
SCA/FR/7.10	It shall have admin module using which administrator(s) can create/edit/delete users and groups	
SCA/FR/7.11	There shall be capability of feature wise blocking - User could be blocked for some activities like forums etc. and still can have access to some services like tax payment.	
SCA/FR/7.12	It shall provide user access logs	
SCA/FR/7.13	Necessary user information like IP, Device ID, time, date of usage etc. shall be captured for audit trail	
SCA/FR/7.14	With regard to interactive services it shall have the following administration features: • Facility to view the list of complaints allocated to the respective field officer • Visibility to problem location's image captured and submitted by the citizen, thereby facilitating field officer with ease of locating the problem area • Real-time monitoring of problem based SLA compared to the defined SLA for each registered complaint allocated to the field officer, thereby allowing better complaint management. • The complaint is color-coded based on their defined SLA status and problem category, red for complaints that crossed SLA period for resolution and green for those complaints that are within SLA. • Facility to change complaint status from 'Open' to 'On Hold' or 'WIP' or 'Close' • Real-time dashboard of operational parameters and highlights areas of concern • Contact book of entire team, to help in reaching out to the right officer instantly for taking appropriate and timely decisions and actions • Mobile work flow alerts and audit related features to RMC/RSCL/RDA employees. • Ability to book key facilities at RMC/RDA	
Application Security		
SCA/FR/7.15	It shall also support latest security certificates like SSL 3.0	
SCA/FR/7.16	If required, application shall have the ability for integration with any active directory server (supporting Lightweight Directory Access Protocol)	
Content Display		

S. No	Minimum Functional Requirements	Compliant (Yes / No)
SCA/FR/7.17	It shall be able to display content with proper formatting	
SCA/FR/7.18	It shall also provide functionality to download documents by the users	
SCA/FR/7.19	Structured overall content with proper tagging to make them screen reader friendly	
SCA/FR/7.20	It shall be ensured that the Mobile Apps adjusts itself automatically as per the screen resolution of the Mobile i.e. 1024*768, 1200*800 etc.	
SCA/FR/7.21	Resolution independent application shall automatically expand/compress itself as per the screen resolution and hence there shall not be any vertical scroll in the Mobile Apps structure	
SCA/FR/7.22	Mobile mirroring for web site, portal, e-governance and other ICT modules. The portal should be mirrored on the mobile (all types of devices and operating systems) for an easy citizen experience. In addition, work flows and alerts to officials shall all be integrated on the mobile device. In line with the National e-Governance Plan objectives	
Other functionalities		
SCA/FR/7.23	The mobile app shall be compatible with iOS and Android mobile platforms and shall be downloaded for free from the appropriate sources.	
SCA/FR/7.24	The application interface shall function with low speed internet connection	
SCA/FR/7.25	It shall be capable of accessing mobile device features like camera, GPS, etc. and must provide directions to desired location selected from the service modules as well as for use by safety service module	
SCA/FR/7.26	The application shall alert the user to download the latest version, which ever available and if required prompt for compulsory upgrade	
SCA/FR/7.27	The application shall be multi-lingual (English, Hindi and Odiya)	
SCA/FR/7.28	Open standards shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices.	
SCA/FR/7.29	Provide mobile-based services through all delivery channels including SMS, Voice/ IVR, Unstructured Supplementary Service Data (USSD), GPRS/3G, SIM Toolkit, and mobile application store (m-Appstore).	
SCA/FR/7.30	For Rourkela Smart City employees and work process enablement of Approval of leave applications, purchase requisitions, payment release, initiate a requisition, work order confirmation etc.	
SCA/FR/7.31	The architecture shall be designed to be robust, reliable and scalable. The architecture as envisaged is that the Portal provides the multi-channel communication interface which drives the mobile apps.	
SCA/FR/7.32	The Portal in turn integrates the e-Governance and other applications which are expected to provide robust functionality which is running at multiple customer sites.	
SCA/FR/7.33	The detailed requirements related to e-Governance and other applications shall be studied and the functionality/business processes shall be detailed out which would be provided on the Portal.	
SCA/FR/7.34	The above mentioned examples should not be assumed as a complete list. The solution architecture of the mobile application must have an end to end business process perspective which cuts across business applications which also demonstrates the quality of resources deployed for preparing the solution design.	

Minimum Technical Requirements

Integrated Multi-Services Digital Kiosks

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
Digital Kiosks		
IDK/TR/1.1	Integrated Multi-Services Digital Kiosks enclosure shall be made of metal or stainless steel fabric and shall be IP 65 rated. It shall be built to last in outdoor environment to support the Project operating conditions.	
IDK/TR/1.2	Metal sheet of the Integrated Multi-Services Digital Kiosks housing shall be made in a minimum 16 gauge that can be powder coated as per the required color choice.	
IDK/TR/1.3	Integrated Multi-Services Digital Kiosks enclosure shall have space to put all the required hardware including switches and associated accessories.	
IDK/TR/1.4	Integrated Multi-Services Digital Kiosks shall have integrated PTZ Camera mounted on the top of the Kiosk Enclosure.	
IDK/TR/1.5	Integrated Multi-Services Digital Kiosks shall also have integrated Wi-Fi access points.	
IDK/TR/1.6	The Integrated Multi-Services Digital Kiosks shall also have integrated solar panel with batteries.	
IDK/TR/1.7	The Integrated Multi-Services Digital Kiosks enclosure shall have integrated receipt printer for taking printout of bills payments receipt and events tickets etc.	
IDK/TR/1.8	The Integrated Multi-Services Digital Kiosks shall have in-built speakers and microphone. Speakers shall be able to deliver clear stereo sound. Microphone shall be able to isolate the main sound source and minimize background noise. At any time, the speakers shall have an output audio of at least 10 dB above ambient noise.	
IDK/TR/1.9	Integrated Multi-Services Digital Kiosks shall have proper ventilation arrangement for heat removal.	
IDK/TR/1.10	Integrated Multi-Services Digital Kiosks shall have proper in-built wiring arrangement with spike proof power socket.	
IDK/TR/1.11	Integrated Multi-Services Digital Kiosks shall have two (2) service doors with security key so that it can be easily accessed from there.	
IDK/TR/1.12	Integrated Multi-Services Digital Kiosks shall be either fixed to ground or have shoes to hold it on a smooth surface.	
IDK/TR/1.13	All electrical components shall have quick-disconnect terminals for easy service or removal. All wiring shall be concealed within the Integrated Multi-Services Digital Kiosks enclosure and shall not be visible from the outside of the unit.	
Interactive User Panel for Information of City Services		
IDK/TR/2.1	The panel shall have built-in capacitive touchscreen for interactive applications with required supporting software for dynamic content management from various sources connected to the system. The content management system shall include content from (but not limited to) – e-governance platform, services billing, Rourkela organized/supported events, digital advertising and promotions (provided as part of the content management system), city news and information, among others.	
IDK/TR/2.2	The touch screen shall be all-glass with a transparent metallic conductive coating.	
IDK/TR/2.3	The touch screen monitor shall have a min. resolution of 1280 x 1024 or better with screen size of minimum 24”.	
IDK/TR/2.4	The screen shall support wide viewing angle, low power consumption, high contrast ratio, high aperture ratio, short response time.	
IDK/TR/2.5	The content displayed on the panel shall be direct sunlight readable and shall support the feature of auto brightness control.	
IDK/TR/2.6	The unit shall have the embedded thin client with quad core CPU 4GB memory, 32 GB Flash, 100 GB of secondary storage for local storage with required OS.	
IDK/TR/2.7	The touch screen monitor shall be capable of withstanding most surface contaminants and must be ASTM-D-1308-02 and ASTM-F-1598-95 compliant.	
IDK/TR/2.8	The touch screen monitor shall be NEMA 4X / IP66 rated and complete water-resistant seal compatible. It shall be capable of operating in outdoor rated environments and shall have a rugged screen.	
Emergency Call Box		
IDK/TR/3.1	The ECB shall be integrated with the Integrated Multi-Services Digital Kiosks and shall be monitored at the ICCC.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
IDK/TR/3.2	At the ICCC, graphical display of the locations of the ECBs mounted on the Integrated Multi-Services Digital Kiosks shall be provided at the workstations to control, configure and manage ECBs at a minimum.	
IDK/TR/3.3	The ECB shall be auto-dial operation and shall be capable of automatically answering incoming calls.	
IDK/TR/3.4	The ECB shall communicate over 10/100/1000 Base TX copper signal ports over Ethernet.	
IDK/TR/3.5	The ECB shall support SIP based Voice over Internet Protocol (VoIP) communications standard.	
IDK/TR/3.6	The ECB shall have network connectivity for monitoring via Web access (HTTP), SNMP, and shall provide the capability of e-mail notification of alarm conditions. Multiple alarms of the conditions shall be provided automatically.	
IDK/TR/3.7	The ECB shall have automatic adjustment of output volume of audio based on ambient noise detection. At any given time, the sound output from ECB speaker shall be 6-10 dB above ambient noise.	
IDK/TR/3.8	The call from ECB shall only be disconnected at the ICCC. The user shall not have the capability to disconnect the call from the ECB itself.	
IDK/TR/3.9	The ECB button shall be circular, red in colour and the panel shall have clear label of 'Emergency Call Button'.	
IDK/TR/3.10	The ECB inside the Integrated Multi-Services Digital Kiosks shall be powered using PoE or PoE+.	
Digital Payments		
IDK/TR/4.1	The Integrated Multi-Services Digital Kiosks shall have the capability for digital payments like electricity bills, water bills, Wi-Fi recharge/coupon, Payment of penalties (Challans, etc.), payment for any city supported events, etc.	
IDK/TR/4.2	The Integrated Multi-Services Digital Kiosks shall accept all digital payments including credit card, debit card and e-wallets.	
IDK/TR/4.3	The Integrated Multi-Services Digital Kiosks shall have option for taking printout of bills payments receipt and events tickets etc. through integrated receipt printer.	
IDK/TR/4.4	The Integrated digital payments for E-Kiosks shall comply with all the revenue/financial departments' norms and conditions for such online financial transactions in India and shall adhered to all such norms and conditions.	
Miscellaneous		
IDK/TR/5.1	The Integrated Multi-Services Digital Kiosks shall be powered by 12/24/48VDC input as per the design requirements to support powering using solar as the primary power. Raw power will be provided for secondary power.	
IDK/TR/5.2	The Integrated Multi-Services Digital Kiosks shall communicate over RJ45, HDMI, DVI and USB.	
IDK/TR/5.3	The Integrated Multi-Services Digital Kiosks shall support operating temperature range as per City requirement	
IDK/TR/5.4	The ECB shall have a MTBF of at least 100,000 hours.	
IDK/TR/5.5	The touch screen monitor shall have a MTBF of at least 50,000 hours.	

Standalone Multi-Services Digital Kiosks

S.No.	Minimum Technical Requirement	Compliant (Yes / No)
Digital Kiosks		
SDK/TR/1.1	Standalone E-Kiosks enclosure shall be made of metal or stainless steel fabric and shall be IP 55 rated.	
SDK/TR/1.2	Metal sheet of the Integrated E-Kiosks housing shall be made in a minimum 16 gauge that can be powder coated as per the required color choice.	
SDK/TR/1.3	Standalone E-Kiosks enclosure shall have space to put all the required hardware including switches (if applicable) and associated accessories.	
SDK/TR/1.4	The Standalone E-Kiosks enclosure shall have integrated receipt printer for taking printout of bills payments receipt and events tickets etc.	
SDK/TR/1.5	The Standalone E-Kiosks shall have proper ventilation arrangement for heat removal.	

S.No.	Minimum Technical Requirement	Compliant (Yes / No)
SDK/TR/1.6	Integrated E-Kiosks shall have proper in-built wiring arrangement with spike proof power socket.	
SDK/TR/1.7	Integrated E-Kiosks shall have two (2) service doors with security key so that it can be easily accessed from there.	
SDK/TR/1.8	Integrated E-Kiosks shall be either fixed to ground or have shoes to hold it on a smooth surface.	
SDK/TR/1.9	All electrical components shall have quick-disconnect terminals for easy service or removal. All wiring shall be concealed within the Integrated E-Kiosks enclosure and shall not be visible from the outside of the unit.	
Interactive user panel for Information of City Services		
SDK/TR/2.1	The panel shall have built-in capacitive touchscreen for interactive applications with required supporting software for dynamic content management from various sources connected to the system. The content management system shall include content from (but not limited to) – e-governance platform, services billing, Rourkela organized/supported events, digital advertising and promotions (provided as part of the content management system), city news and information, among others.	
SDK/TR/2.2	The touch screen shall be all-glass with a transparent metallic conductive coating.	
SDK/TR/2.3	The touch screen monitor shall have a min. resolution of 1280 x 1024 or better with screen size of minimum 24”.	
SDK/TR/2.4	The screen shall support wide viewing angle, low power consumption, high contrast ratio, high aperture ratio, short response time.	
SDK/TR/2.5	The content displayed on the panel shall be direct sunlight readable and shall support the feature of auto brightness control.	
SDK/TR/2.6	The unit shall have the embedded thin client with quad core CPU 4GB memory, 32 GB Flash, 100 GB of secondary storage for local storage with required OS.	
SDK/TR/2.7	The touch screen monitor shall be capable of withstanding most surface contaminants and must be ASTM-D-1308-02 and ASTM-F-1598-95 compliant.	
SDK/TR/2.8	The touch screen monitor shall be NEMA 4X / IP66 rated and complete water-resistant seal compatible. It shall be capable of operating in outdoor rated environments and shall have a rugged screen.	
Digital Payments		
SDK/TR/3.1	The Standalone E-Kiosks shall have the capability for digital payments like electricity bills, water bills, Wi-Fi recharge/coupon, Payment of penalties (Challans, etc.), payment for any city supported events, etc.	
SDK/TR/3.2	The Standalone E-Kiosks shall accept all digital payments including credit card, debit card, e-wallets and Internet Banking.	
SDK/TR/3.3	The Standalone E-Kiosks shall have option for taking printout of bills payments receipt and events tickets etc. through integrated receipt printer.	
SDK/TR/3.4	The Standalone digital payments for E-Kiosks shall comply with all the revenue/financial departments’ norms and conditions for such online financial transactions in India and shall adhered to all such norms and conditions.	
Miscellaneous		
SDK/TR/4.1	The Stand-alone Multi-Services Digital Kiosk shall be powered by raw power, 220V at 50 Hz. Any power conversion and UPS requirements shall be in scope of Bidder.	
SDK/TR/4.2	The Standalone E-Kiosks shall communicate over RJ45, HDMI, DVI and USB.	
SDK/TR/4.3	The Standalone E-Kiosks shall support operating temperature range as per City requirement	
SDK/TR/4.4	The touch screen monitor shall have a MTBF of at least 50,000 hours.	
SDK/TR/4.5	Connectivity requirements of Stand-alone Multi-Services Digital Kiosks shall be met by Ethernet as well as 3G/LTE	

Mobile App

S.No.	Minimum Technical Requirement	Compliant (Yes / No)
Start-up time		
SCR/TR/1.1	The start-up time of the application should be less than 5 seconds	
Responsiveness		

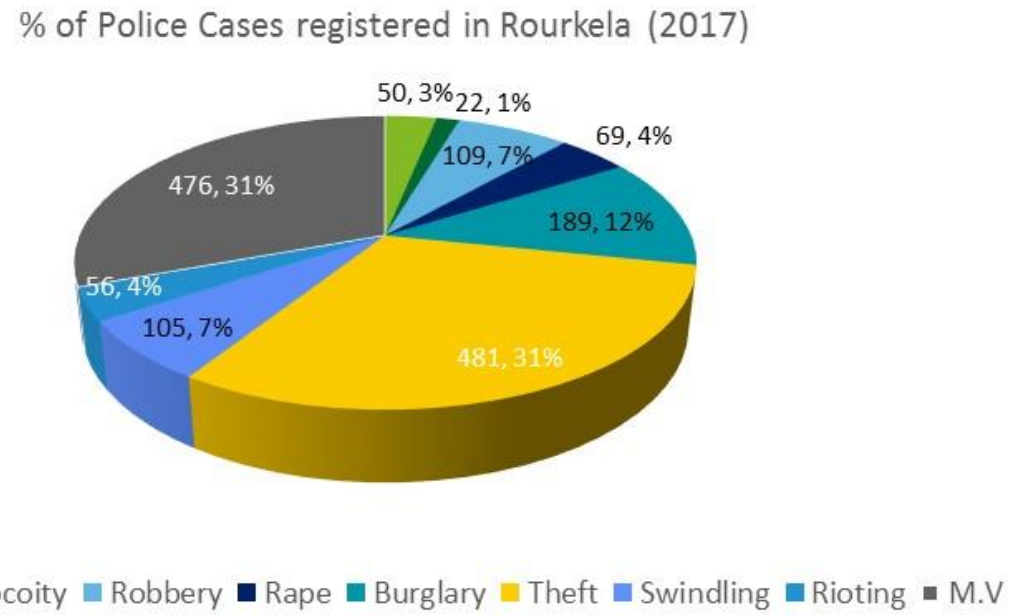
S.No.	Minimum Technical Requirement	Compliant (Yes / No)
SCR/TR/2.1	The application should render properly on all devices of different size and resolution (i.e. it should support all standard resolutions)	
Memory		
SCR/TR/3.1	App should support devices having memory capacity of minimum 1 GB	
Battery Life		
SCR/TR/4.1	The mobile application should be developed using standard SDKs of Android and iOS along with battery life saving APIs such that app consumes minimum battery of device including features such as: • Request data once and use multiple times for different operations • Caching • Less download and perform one large operation v/s number of small ones	
Support for different Network channels		
SCR/TR/5.1	The application should support different network channels like Wi-Fi, 2G, 3G & 4G and the application should be able to run on low bandwidth	
Interruption, notifications and multi-tasking		
SCR/TR/6.1	The application should not come in the way of the mobile's operating system processing the user's decision to respond to the interrupt (such as accepting a call or reading an SMS), and it should not result in any damage to application's ability to function normally after the operating system resumes application after the user finishes handling the interrupt or after they choose to ignore the interrupt.	
Maintainability and Change in Module		
SCR/TR/7.1	Technical design should not be monolithic in such a way that any change/repair of a single module affects entire application which needs to be tested every time. Design should be modular so that only changed module needs to be deployed and tested.	

Safety and Surveillance

Context

Rourkela is currently served by 24 police stations located across the city. The city accounts for 3% of total registered police cases in the State. Among the cases registered, a high number of cases are on account of Theft and Motor Vehicle Accidents (31% each of total no. of registered cases).

Presently, there is no full-fledged city surveillance system across the city and the Office of Superintendent of Police (SP Office) currently monitors select locations, including parts of Udit Nagar, Basanti colony and Civil Township through CCTV surveillance on a pilot basis. A total of 36 Fixed cameras and 6 PTZ cameras have been deployed across these locations which are integrated to a control centre situated at the SP Office. Some of the key issues identified in absence of a dedicated pan city wide surveillance system has been presented below.



- High number of registered cases on account of Theft and Motor Vehicle Accidents (31% each of total no. of registered cases)
- Lack of surveillance cameras on a Pan City basis results in delays in crime detection and response
- Riots and vandalisms goes undetected on a real time basis in lieu of absence of CCTV cameras at important places
- Currently, the citizens do not have access to a dedicated Emergency Response System

In order to improve the surveillance reach and response efficiency of the city police, it is imperative to have a pan city network of surveillance cameras for time-bound and efficient mitigation of crime across the city.

Objective

The overall objective of a city surveillance system is to enhance monitoring and management of incidents in the city through CCTV camera based surveillance network. The system shall create a supporting mechanism for the city law enforcement agencies through 24x7 surveillance and monitoring throughout the city as well as enable proactive identification of security issues leveraging intelligent analytics from the surveillance system. Key objectives of the system are as follows:

- Supporting law enforcement agencies in 24x7 surveillance and monitoring
- Proactive identification of security issues leveraging intelligent analytics from the surveillance system
- Implementing a structured and effective process for emergency response and incident management
- Supporting active response during emergency & disaster situations

Scope of Work

The broad scope of work to be covered under this sub module shall include the following, but is not limited to:

- The MSI shall design, supply, and install the surveillance cameras as defined in the RFP; all wiring connections for the system shall be installed by the MSI. The MSI shall supply all of the necessary equipment for the camera operations including camera housings and mountings, camera poles, switches, cabling, and shall make the final connections to the junction box.
- The MSI shall undertake due diligence for selection and placement of surveillance cameras to ensure the optimized coverage of the traffic junction and other locations along with all associated junction arms, accuracy of the information captured on the field and for rugged operations.
- The MSI shall be responsible for providing the entire necessary IT infrastructure for monitoring, recording, storage & retrieval of the video streams at viewing centers, ICCC or any other location as specified in the RFP.

The MSI shall install Surveillance System Cameras for CCTV monitoring and management at 110 locations as given in the table below across the Rourkela city.

No.	Area	Location
1.	Ring Road	Birsa Square
2.	Ring Road	Saw Mill Square
3.	Ring Road	IG Park Traffic Tower
4.	Ring Road	Sector-2, DAV College Square
5.	Ring Road	Sector-2, Bus Stand Square
6.	Ring Road	Sector-3, Square
7.	Ring Road	Sector-20, Pani Tanki Square
8.	Ring Road	Sector-20
9.	Ring Road	VIP Road Square
10.	Ring Road	Ambagan Square
11.	Ring Road	Sector-06 Square
12.	Ring Road	Sector-7/17 Square
13.	Ring Road	Sector 08 Square (Jublee Park)
14.	Ring Road	DPS School Square, Sector-14
15.	Ring Road	Space Chowk
16.	Ring Road	Abhigyan Chowk
17.	Ring Road	SOS Village Chowk
18.	Ring Road	DAV School (Boat) Chowk
19.	Ring Road	Hanuman Vatika

No.	Area	Location
20.	Ring Road	Sarana Chowk
21.	Ring Road	Satala Chowk
22.	Ring Road	Traffic Chowk
23.	Main road	Panposh Gandhi Chowk
24.	Main road	Govt. College
25.	Main road	ITI Chowk
26.	Main road	STI Chowk
27.	Main road	Court (Birajapallli)
28.	Main road	SP Office
29.	Main road	Ambedkar Chowk
30.	Main road	Malgodam
31.	Main road	Mangal Bhawan Lane
32.	Main road	Daily Market (Town High School)
33.	Main road	Plant Site
34.	Main road	Glamour Chowk
35.	Main road	Orissa Bastra Bhandar
36.	Main road	Big Bazar Chowk
37.	Main road	Old Taxi Stand
38.	Main road	Madhusudan Chowk
39.	Main road	Railway Station Square
40.	Main road	Gandhi Road
41.	Main road	Gurudwara
42.	Main road	New Bus Stand
43.	Civil Township	Lifeline Chowk
44.	Civil Township	Cakery Bakery Chowk
45.	Civil Township	SBI Trg. Center Chowk

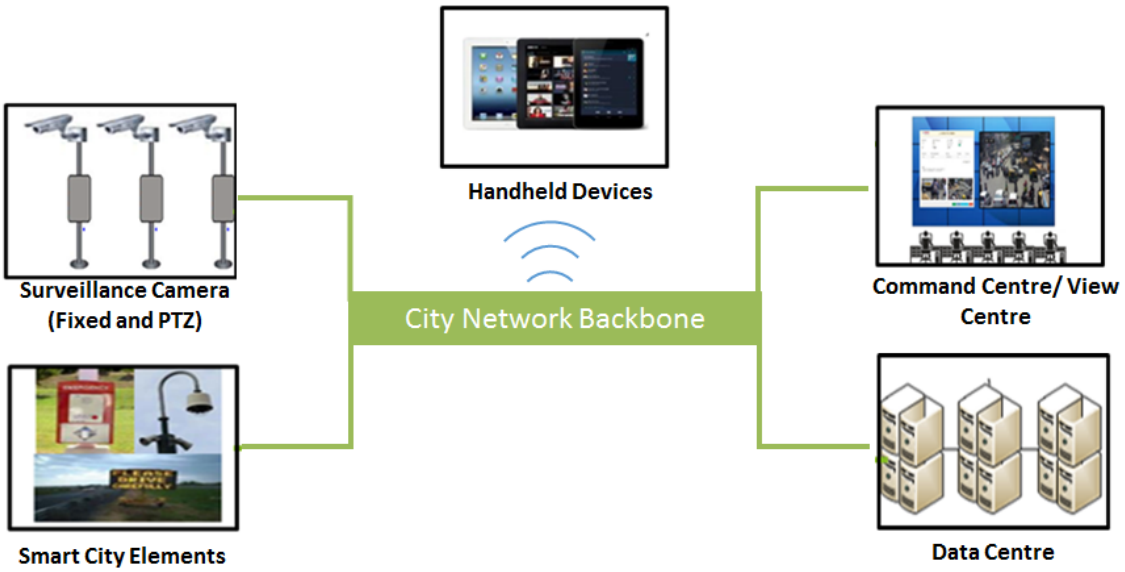
No.	Area	Location
46.	Civil Township	Sub-Divisional Hospital, Panposh
47.	Civil Township	Friday Market, Panposh
48.	Civil Township	Sport Hostel, Panposh
49.	Civil Township	Hi-Tech byPass
50.	Civil Township	A4/1 Front
51.	Mahtab Road	Hockey Chowk
52.	Mahtab Road	Ambika Bisra Munda Chowk
53.	Mahtab Road	DN Patel Chowk
54.	Mahtab Road	RGH Chowk
55.	Mahtab Road	RMC/ WESCO Chowk
56.	Mahtab Road	IDGAH/ Janta Niwas Gali
57.	Mahtab Road	Power House Road
58.	Mahtab Road	Indira Gandhi Chowk
59.	Mahtab Road	Indian Boiler Chowk
60.	Chhend	VSS Market Chhend
61.	Chhend	Chinmaya School
62.	Chhend	RIMS Chowk
63.	Chhend	BSNL Chowk
64.	Chhend	Biju Pattanaik Chowk
65.	Chhend	Tulasitola
66.	Chhend	Cooperative Colony Chowk
67.	Chhend	Jail Chowk
68.	Chhend	H.K Ray College Road
69.	Koel Nagar	Hill Top
70.	Koel Nagar	Koel Nagar D/E
71.	Koel Nagar	Koel Nagar D/A, Jagannath Temple

No.	Area	Location
72.	Koel Nagar	Jhirpani Police Station
73.	Koel Nagar	Koel Nagar B.C Block
74.	Koel Nagar	Koel Nagar Tarini Mandir Chowk
75.	Koel Nagar	Mahapatra Market Complex
76.	Koel Nagar	Shakti Nagar Chowk
77.	Koel Nagar	Prativa Computer
78.	Koel Nagar	Sarna Chowk, Jagda
79.	Koel Nagar	BSNL/CWS/ NIT Back Gali
80.	Koel Nagar	NAC market near shiv temple
81.	Koel Nagar	NIT Main Gali
82.	Fertiliser Township	Deogaon (Gandhi College)
83.	Fertiliser Township	Rangila Square
84.	Fertiliser Township	Jalda C
85.	Fertiliser Township	Naba Krushan Nagar, Chowk
86.	Basanti Colony	Baji Rout
87.	Basanti Colony	Malgodam
88.	Basanti Colony	DL Chowk
89.	Basanti to BSNL Chowk	Railway Colony Bazar
90.	Basanti to BSNL Chowk	Gopabandhupali Railway Station
91.	Basanti to BSNL Chowk	BSNL Chowk
92.	Civil Township	Chamber of Commerce
93.	Main road	Income Tax Office
94.	Mahtab Road	Max Gali towards railway station
95.	Mahtab Road	Bhati road
96.	Ring Road	Sail Chowk
97.	Bondamunda	Tilkanagar Chowk

No.	Area	Location
98.	Bondamunda	Sector-A Chowk
99.	Bondamunda	Sector-C Chowk
100.	Bondamunda	D Cabin Chowk
101.	Bondamunda	Dumerta Chowk
102.	Bondamunda	Koilagate Chowk
103.	NH 10	NH RCCF office Chowk
104.	Civil Township	Subhash Park
105.	Main road	Udit Nagar Parade ground
106.	Civil Township	Rotary Park
107.	Ring Road	Birsa Stadium
108.	Main road	One stop Rourkela
109.	Ring Road	IG Park Main gate
110.	Ring Road	Bhanja bahwan

Indicative Solution Architecture

An indicative solution architecture proposed for the installation of city surveillance system to enhance monitoring and management of incidents in the city is presented in the figure below:



As highlighted in the figure above the network comprises of network of CCTV cameras, which are connected to network video recorder (NVR) which stores and converts the video input as per the output requirement. The converted video feed is relayed to the ICCC, which is monitored by operators. On the event of detection of an incidence or possible cause of event, an alert is generated. Based upon the nature of alert the operator informs the concerned department for their timely response and resolve of the incident.

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. General		
Safety/FR/1.01	RSCL's City Surveillance and Service monitoring System shall consist of but not limited to : • Fixed Cameras • PTZ Cameras • Infrared Illuminators • Network Video Recorder (NVR) • Video Management System (VMS) • Intelligent Video Analytics • Camera Accessories i.e. Power Supplies, Cable, Connectors and associated accessories for an integrated system	
Safety/FR/1.02	The cameras implemented as part of this Project shall be rated for operations in outdoor environment (for outdoor installations) and depending on the objective/application, shall be of different configurations including PTZ or fixed cameras	
Safety/FR/1.03	All the Cameras shall be IP based	
Safety/FR/1.04	The CCTV surveillance system shall be Open Network Video Interface Forum (ONVIF) compliant	
Safety/FR/1.05	Cameras shall have an integral receiver/driver that shall be capable of controlling pan-tilt, zoom and focus locally and also remotely from the Integrated Command & Control Centre (ICCC)	
Safety/FR/1.06	All cameras shall support real-time video content analysis	
Safety/FR/1.07	All cameras shall be installed on existing poles. New poles will be erected as per requirement	
Safety/FR/1.08	Indicative list of capabilities of RSCL's Safety and Surveillance system are as follows: • Real-time monitoring of City • Event based monitoring of City • Providing secured access to video at any time from any network location • Situation/Rule based alerts based on user inputs • Automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies; • Access to historic video data for investigative purposes	
2. Cameras		
Safety/FR/2.01	The surveillance system shall support following Analytics based on Artificial Intelligence having min 80% accurecy for the Cameras on edge devices: • Auto Tracker: To detect and track movement in the field of view • Adaptive Motion Detection: To detect and track object that enter a scene and then triggers an alarm when the object enter a user-defined zone • Abandoned Object: To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allow • Camera Sabotage: Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap • Directional Motion: Generates an alarm in a high traffic area when a person or object moves in a specified direction • Object Removal: To triggers an alarm if the object is removed from a user-defined zone • Stopped Vehicle: To detect vehicles stopped near a sensitive area longer than the user-defined time allows • Intrusion Detection – Detect intrusion	
Safety/FR/2.02	Event (alarm) Handling:	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	• The camera shall be capable of recording an event as pre and post event images to on-board SD Media Card and on Network Video Recorder (NVR). Events may be triggered using camera motion detection or from an external device input such as a relay • When triggered from an external input or the camera's motion detector, the camera shall be capable of sending JPEG images via e-mail and/or sequences of images to an FTP server or on-board compact flash and NVR • A relay output shall be available upon the activation of the camera's motion detector or external relay input. The relay output may also be manually activated from the live view screen	
Safety/FR/2.03	The system shall allow classification of different objects like animals, vehicles, people etc.,	
Safety/FR/2.04	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.	
Safety/FR/2.05	VCA shall provide secured feeds with encryption, watermarking for data authenticity	
Safety/FR/2.06	VCA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.,	
Safety/FR/2.07	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system	
Safety/FR/2.08	VAS should allow to add, edit, delete or disable and enable Policies.	
Safety/FR/2.09	The city wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1: • Parking Violation • Wrong Direction • People loitering • Unattended Object • Crowd detection • People tracking	
Safety/FR/2.10	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)	
Safety/FR/2.11	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification,	
Safety/FR/2.12	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.	
3. Facial Recognition System		
Safety/FR/3.01	The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system.	
Safety/FR/3.02	The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator	
Safety/FR/3.03	The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real time report such as Audit log report, Hit List Report, Daily Statistics Report, and Distribution Report.	
Safety/FR/3.04	The facial recognition system should be accessible from 5 different desktop/ laptops at any given time. When choosing a distributed architecture, the system shall be	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision.	
Safety/FR/3.05	The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts.	
Safety/FR/3.06	The algorithm for facial recognition or the forensic tool should be able to recognize partial faces with varying angles	
Safety/FR/3.07	The system should be able to detect multiple faces from live single video feed	
Safety/FR/3.08	The system should have combination of eye-zone extraction and facial recognition	
Safety/FR/3.09	The system should have short processing time and high recognition rate	
Safety/FR/3.10	The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)	
Safety/FR/3.11	Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall make use of GPU technology with artificial intelligence with continuous improvement instead of Traditional CPUs and Computer vision, to greatly improve the computational performance in crowded environments.	
Safety/FR/3.12	The system should be able to identify and authenticate based on individual facial features	
Safety/FR/3.13	The system should be compatible with the video management system being proposed by the system integrator	
Safety/FR/3.14	The system should have capability for 1:1 verification and 1:N identification matching	
Safety /FR/3.15	The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.	
Safety /FR/3.16	The system should be able to support diverse industry standard graphic and video formats as well as live cameras	
Safety /FR/3.17	The system should be able to match faces from recorded media.	
Safety /FR/3.18	The system should be able to detect a face from a group photo	
Safety /FR/3.19	The system should be able to detect a face from stored videos of any format	
Safety /FR/3.20	The system should have bulk process of adding faces in the system	
Safety /FR/3.21	The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing. OS to capture a face on the field and get the matching result from the backend server.	
Safety /FR/3.22	The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas.	
Safety /FR/3.23	The system shall be able to detect faces in different environmental changes like rain, wind, fog and poor light.	
4. Network Video Recorder (NVR)		
Safety/FR/4.01	NVRs shall be sized to provide minimum 30 days storage assuming recording of 24hrs a day, 7 days a week and 30 days a month at 4 CIF resolution. All NVRs shall be provided in an N+N configuration	
Safety/FR/4.02	NVRs shall have in-built capabilities of recording video and audio streams directly from IP based cameras installed at field	
Safety/FR/4.03	NVRs shall be ONVIF compliant	
Safety/FR/4.04	NVRs shall be capable of reviewing video and audio streams on-demand using the supplied central software	
Safety/FR/4.05	NVRs shall be capable of storing all alarms generated as part of the CCTV surveillance system	
Safety/FR/4.06	NVRs shall be capable of supporting all recording of camera analytics	
Safety/FR/4.07	NVRs shall be network enabled for remote access, viewing, management and status monitoring. User Name and Password protection is required for access. The system	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	must provide for remote administrator management of user names, passwords and management of definable end user rights	
Safety/FR/4.08	A network user/client interface software shall be supplied at no cost to RSCL. The functional requirements of this client interface software will be reviewed and approved by RSCL or their designate	
Safety/FR/4.09	NVR Unit(s) shall provide fully configurable recording options to include, but not limited to: • Full record • Record on motion only • Variable frame rate • Variable resolution • Change of recording configurations on receipt of an alarm globally and/or per camera • Enable audio recording on receipt of an alarm	
5. Recording and Storage		
Safety/FR/5.01	The storage solution proposed should be such that the video feeds are available for 30 days. After 30 days, the video feeds would be overwritten or archived unless they are flagged or marked by the Police or RSCL for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police or RSCL deem it good for deletion	
Safety/FR/5.02	For incidents that are flagged by the Police, RSCL or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted	
Safety/FR/5.03	The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line	
Safety/FR/5.04	The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices	
Safety/FR/5.05	The system shall support H.264, H.265 or better, MPEG-4 and MJPEG compression formats for all IP cameras connected to the system.	
Safety/FR/5.06	The system should not limit amount of storage to be allocated for each connected device.	
Safety/FR/5.07	The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously. The system shall support archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.	
Safety/FR/5.08	Bandwidth optimization - The Recording Server / System shall offer different codec (H.264, H.265, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems	
Safety/FR/5.09	From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server	
Safety/FR/5.10	The Recording Server / System shall support Camera devices from various manufacturers	
Safety/FR/5.11	The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
Safety/FR/5.12	The system shall support full two-way audio between Client systems and remote devices i.e. CCTV	
Safety/FR/5.13	Failover Support - The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online. The system shall support multiple Failover Servers for a group of Recording Servers	
Safety/FR/5.14	SNMP Support - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system. The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions	

6. Video Management System (VMS)

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.01	Central software application to be installed at the ICCC shall be able to run on any PC based on standard operating systems and shall be license free.	
Safety/FR/6.02	Video Management System (VMS) shall be non-proprietary and open-ended to support integration with ICCC platform and analytics platform.	
Safety/FR/6.03	Central Application Server shall allow user to view live video stream.	
Safety/FR/6.04	Software shall consist of a single client application and the client software shall not be dependent on, nor require any connection to, a central management or configuration server.	
Safety/FR/6.05	The client software shall be installable without any need for software or hardware license.	
Safety/FR/6.06	Dockable windows shall include: • Site Explorer • Alarms/Events window • PTZ and advanced telemetry functions • Monitors window • Maps window	
Safety/FR/6.07	The system shall support a distributed architecture with no single point of failure.	
Safety/FR/6.08	Video shall normally stream direct from camera to client; streaming via a proxy, or intermediate server shall not be the normal function of the system but may be selected as an option.	
Safety/FR/6.09	A client need not ask “permission” to connect to a camera. The handshake between client and camera shall be done directly.	
Safety/FR/6.10	There shall be no single management server. System management shall be distributed throughout the system.	
Safety/FR/6.11	Recording failover shall be standard without need for additional license and/or hardware.	
Safety/FR/6.12	RSCL’s workstations should remain “connected” to all recording devices simultaneously.	
Safety/FR/6.13	Video shall normally stream direct from camera to client; streaming via a proxy, or intermediate server shall not be the normal function of the system but may be selected as an option.	
Safety/FR/6.14	VMS shall allow the overlay of time and date and site information on live video panes, either on all panes, or selected pane only. In addition, the overlay may consist of a user-provided transparent PNG or JPEG file.	
Safety/FR/6.15	VMS shall allow users to view live video and review recorded video at the same time.	
Safety/FR/6.16	VMS shall be ONVIF compliant.	
Safety/FR/6.17	Users shall be able to display any camera view (virtual preset) and Administrators shall be able to configure hidden zones on fixed cameras.	
Safety/FR/6.18	VMS shall allow users to reveal the hidden zone in live video if the user has the appropriate permission.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.19	Users shall be able to save the current zoom/scroll position as a camera view (virtual preset).	
Safety/FR/6.20	VMS shall allow the display of analytics levels on video wall.	
Safety/FR/6.21	Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images.	
Safety/FR/6.22	Users shall be able to print a snapshot of an image displayed in a video pane direct on a printer (colour or grayscale, depending on printer).	
Safety/FR/6.23	Users shall be able to replay currently viewed live video by a single mouse click for replays from 10, 15 or 30 seconds before current time or from alarm time.	
Safety/FR/6.24	Users shall be able to configure the size for text and icons displayed on video panes. Text and icons can be fixed size or adjust automatically when video pane size changes.	
Safety/FR/6.25	In the event of the video connection failing, Shall display a clear error message with the option to also display the last video frame received.	
Safety/FR/6.26	Event Counting: Shall allow users to view a count of analytics events on the video pane while video is being displayed. Shall allow users to reset the event count for a camera.	
Safety/FR/6.27	**Analog and Digital inputs to be displayed on OSD:** The VMS will be able to display be display analog and digital camera information on the OSD • Camera Name • Date and Time Shall support point to point connections for the following data • Video (SD Only) • Audio transmit and receive • Serial	
Safety/FR/6.28	**Audio in Live Video:** • Users shall be able to listen to audio from multiple cameras through PC speakers. • Users shall be able to speak to one or more cameras through a PC microphone. • Users shall be able to listen to audio from a camera through monitor's speakers. • Users shall be able to speak to a camera displayed on monitor through a microphone connected to a decoder. • Users shall be able to mute a client speaker. • Shall have an option to allow or prevent simultaneous listen and speak (full duplex audio). If full duplex audio is off, the direction of audio will be switched automatically when the user listens or speaks. • Users shall be able to listen to audio streams that do not have associated video.	
Safety/FR/6.29	**PTZ Control:** • All PTZ control shall be user-restricted. • Users shall be able to configure named preset positions with optional "tool tip" text. • Users shall be able to configure named custom commands with optional "tool tip" text. Commands can be per PTZ type or per camera, as required. • Users shall be able to copy custom PTZ commands from one camera to another. • Users shall be able to simultaneously pan and tilt a PTZ camera displayed in a video pane in any direction and at varying speed by moving the PC mouse on the video pane. • Users shall be able to zoom a PTZ camera in or out using the PC mouse. • Users shall be able to simultaneously pan, tilt and zoom a PTZ camera displayed in a video pane or monitor using a joy stick on one of the supported CCTV keyboards.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)

	• Users shall be able to adjust the focus of a PTZ camera using the on screen PTZ controls or a CCTV keyboard:
	  - Focus near
	  - Focus far
	  - Auto-focus
	• Users shall be able to adjust the iris of a PTZ camera using the on screen PTZ controls or a CCTV keyboard: Open iris-Close-Auto-iris.
	• Users shall be able to move a PTZ camera to a preset position using the on screen PTZ controls or a CCTV keyboard.
	• Users shall be able to perform a custom command on a PTZ camera using the on screen PTZ controls (e.g. operate wipers.).
	• Users shall be able to enter the menu on a PTZ camera using the on screen PTZ controls or a CCTV keyboard (menu options navigated using pan and tilt.).
	• Shall automatically drop the connection to a PTZ camera if not moved for 5 seconds to allow other users to control it.
	• Users shall be able to hold onto connections to PTZ cameras to prevent other users taking control if not moved (overrides the 5 second timeout.).
	• Users shall be able to take control of a PTZ camera if user has a higher priority than the user currently moving it (overrides PTZ hold.).
	• Inform user when can't take control of a PTZ camera because another user with a higher priority is controlling it.
	• Users shall be able to show or hide the on screen PTZ controls.
	• Shall support the following for cameras using the ONVIF interface or Camera Gateway:
	  - Pan, tilt and zoom control with mouse and joystick.
	  - Go to preset
	  - Set preset	

Safety/FR/6.30	**Timeline and Calendar:** • Users shall be able to view the recorded video footage for a camera along a timeline. They shall be able to expand and contract the timeline to show a larger or smaller time range and to scroll the timeline backwards and forwards to show different time periods. • For a camera, users shall be able to see summary information about how much recording footage is available from which NVR. • Users shall be able to change the playback NVR associated with a camera. • Shall provide one-button click controls to go to the beginning or the end of available recording footage. • Shall provide a calendar control to allow navigation to any year / month /day in the recording library. • Shall provide a go to “hour / minute / second” control. • Shall display alarms related to the selected camera along the timeline including summary counts of the number of alarms in each time period. • Shall display video bookmarks along the timeline. Bookmarks can either be those from a selected camera or from current bookmark query as displayed in the bookmark list.	
Safety/FR/6.31	**Playback on PC Screen or Video Wall:** • Shall play back video recorded in MJPEG, MPEG4 and H.264, H.265 formats or better. • Shall replay footage in same video pane, or navigate to recorded video panes. • Shall play back video Min. of 25 cameras at once in a single video window. • Shall play back each camera separately or synchronize to playback from the same time. • Shall play back synchronized recorded audio in each video pane. • Shall display time and date information on recorded video panes, either on all video panes, or on the selected pane only. This should be able to be set independently of the settings for live video panes.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• Shall play back video using the following standard VCR operations: • Play-pause-fast forward at different speeds. • Rewind at different speeds. • Single frame forward-single frame back. • Shall provide a jog shuttle speed control for fast forward and rewind. • Users shall be able to move playback to a different time either using the timeline or entering a specific date and time. • Users shall be able to move playback to the time of the next alarm, bookmark or motion over threshold. • Users shall be able to move playback to the time of the previous alarm, bookmark or motion over threshold. • Users shall be able to digitally zoom up to 1000% and scroll replayed video. • Users shall be able to reveal the hidden zone in recorded video if user has the appropriate permission. • Users shall be able to remove interlacing artefacts from 4CIF video • Users shall be able to display analytics levels on video. • Users shall be able to take a snapshot of one image or all images currently displayed and save as a bitmap or JPEG image to a configurable location. This should include zoomed images. • Users shall be able to print a snapshot of an image displayed in a video pane direct to a printer (colour or grayscale, depending on printer).	
Safety/FR/6.32	**Motion Search:** • Users shall be able to find motion in recorded footage from a selected time and display a motion profile on the timeline. • Users shall be able to adjust the motion threshold used for thumbnails and for moving playback to next/previous motion. • It shall be possible to combine motion search modes to further refine the search. • Users shall be able to adjust the speed and granularity of the motion search.	
Safety/FR/6.33	**Audio Search:** • Users shall be able to search for sounds in recorded footage from a selected time and display an audio level profile on the timeline. • Users shall be able to adjust the audio threshold used for thumbnails and for moving playback to next/previous sound.	
Safety/FR/6.34	**Thumbnails** Shall be able to display thumbnail images taken from the video footage in the current time line period. Thumbnails can be displayed by: • Time: At equal intervals across the timeline period depending. • Alarms: One image for each alarm in the period. • Bookmark: One image for each bookmark in the period. • Motion: One image for each time motion goes above a configurable threshold. • Audio: One image for each time the audio goes above a configurable threshold. • Users shall be able to play back a recording from a selected thumbnail on the number of thumbnails set for the use.	

Safety/FR/6.35	**Bookmarks:**
	• Users shall be able to add a bookmark to a recording for a camera at a specified time.
	• Users shall be able to find bookmarks by:
	  • Site name.
	  • Camera name.
	  • Time range.
	  • A text string within the bookmark.
	• Users shall be able to produce reports of bookmarks and export to RTF or CSV formats.
	• Users shall be able to delete one or more bookmarks (if created by the same user).	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• Users shall be able to delete bookmarks created by any user. • Shall ensure that bookmarks are held alongside recordings on the NVR, not on a user's PC. • Users shall be able to view recorded video associated with a bookmark. • It shall be possible for text information to be automatically fed into the IP Video System as Bookmarks via an SDK. • Shall ensure that the text information is displayed in a scrolling bookmark comments window beside the playback window. • Detailed search options shall allow for filtering of bookmarks e.g. by time, by user. • Within the bookmark comments window the highlighted bookmark shall correspond to the current playback position. • Next and previous incident buttons shall automatically scroll the bookmark comments window keeping the highlighted text and associated video in synch. • In a live view pane, users shall be able to add a bookmark to the recording of that camera. • Users shall be able to view bookmarks as a transparent overlay on a live pane. • Shall support permissions for bookmarks so that only those users with the appropriate security level can view bookmarks created by users at the same level as them or below.	
Safety/FR/6.36	**Incident Export:** • Users shall be able to export video clips from a selected camera or cameras within a site to a named incident. • Users shall be able to select the start and end times of the export by clicking and dragging on the timeline. • Time to export shall be no more than 30 seconds per hour of video recorded. • Users shall be able to queue video exports to be performed as a background process. • Shall show progress and estimated time to completion in an export status window • Users shall be able to a.dd additional clips to existing incidents. • Shall automatically digitally sign video clips on export. • Users shall be able to protect the original recordings to preserve the evidence. • Users shall be able to review incidents in a standalone incident player application, directly from CD. • Users shall be able to play back incidents with all the Playback operations provided by the full Video Management System application. • Users shall be able to check and authenticate digital watermarks embedded within exported clips. • The Incident Player application shall be able to be run at the same time as the main Video Management System application so that users can easily verify the success of an export. • Shall support the following ONVIF cameras and cameras streamed via Camera Gateway: • Export of video recorded in MJPEG, MPEG4,and H.264,H.265 • Playback of exported video in exported player. • Shall provide the option to include date and time on each frame of the recording when it is exported. • Administrators shall have the ability to restrict the location that users may export video files.	
Safety/FR/6.37	• Users shall have the ability to produce a simple easy to view video summary of an incident. • Users shall have the ability to export all video associated with this summary. • All video in this export should be fully watermarked.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• The GUI shall allow addition, removal and edit of clips involved in the summary. This editing should be done via GUI.	
Safety/FR/6.38	**Playback on Monitors:** • Users shall be able to play back recorded video on monitor from a selected time • Shall support basic play back operations on monitor: • Play • Pause	
Safety/FR/6.39	**Audio in Playback:** • Users shall be able to listen to audio recorded with video from all cameras being played back or selected cameras only. • Users shall be able to listen to audio streams without the need to display anything in the video pane. • Shall support the following for 3rd Party cameras through ONVIF: • Listen to recorded audio.	
Safety/FR/6.40	Users shall be able to start an instant recording from live video viewed in a video pane. They shall have the option to start recording video only or both video and audio.	
Safety/FR/6.41	• Users shall be able to configure the recording schedule for cameras on NVRs. Recording can be configured to be: • 24/7 • Timed (from minute to weekly schedules) • On alarm or event	
Safety/FR/6.42	Users shall be able to specify the transport protocol to be used for recording (TCP, UDP, and Multicast).	
Safety/FR/6.43	Users shall be able to specify whether audio should be recorded with the video.	
Safety/FR/6.44	Users shall be able to specify whether the recording should be protected when an alarm or event occurs (from a specified time before the alarm / event).	
Safety/FR/6.45	Users with appropriate permissions shall be able to enable or disable recordings temporarily.	
Safety/FR/6.46	Users shall be able to delete recording schedules.	
Safety/FR/6.47	Users shall be able to copy recording schedules from one camera to other cameras on the same or another NVR.	
Safety/FR/6.48	Users shall be able to specify an alternative NVR to record to during a video “lockout” for either a camera or a site. Lockout permission can be used to prevent all other users from viewing and recording from a selected camera or all cameras in a selected site.	
Safety/FR/6.49	Shall support digital signing (watermarking) of recordings as they are recorded on the NVR.	
Safety/FR/6.50	Users shall be able to find recordings within a specified time period.	
Safety/FR/6.51	Users shall be able to protect/unprotect recordings.	
Safety/FR/6.52	Shall display a warning message if an NVR is unable to retain the number of days recording for which it was configured.	
Safety/FR/6.53	Shall support the configuration of failover NVRs for each primary NVR with the following options: • 1 to N: 1 primary NVR can have one or more failover NVRs. • N to 1: multiple primary NVRs can have the same failover NVR. • Continuous recording to primary and failover NVRs. • Recording to failover NVR only when primary NVR fails.	
Safety/FR/6.54	Shall automatically failover when a primary NVR is down.	
Safety/FR/6.55	In addition, users shall have the option to manually failover, for example to allow for routine maintenance of a primary NVR.	
Safety/FR/6.56	Users shall have the option to manually fail back to a primary NVR, with the option to restore the recording configuration from the failover NVR to the primary.	
Safety/FR/6.57	Shall support binary inputs on IP Cameras, encoders, decoders and alarm panels, video loss alarm inputs, network loss alarm inputs and NVR fault alarm inputs, analytics alarm inputs as separate flag and including: • Raid degraded	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• License failure • Recording failure • Redundant power failure	
Safety/FR/6.58	Shall support • Alarm inputs from 3rd party systems. • Multiple alarm inputs (detectors) to be grouped into an alarm zone. • Inputs (detectors) that do not cause an alarm to be generated.	
Safety/FR/6.59	Shall support 'AND' logic between detectors so that the alarm input is activated only when both detectors are activated with a defined time period.	
Safety/FR/6.60	Shall support detectors that are activated and deactivated by different inputs e.g. activate on a binary input from one device and deactivate on a binary input from another device.	
Safety/FR/6.61	Ability to sort the alarm information in various ways in GUI.	
Safety/FR/6.62	Shall support set and unset of alarm zones such that alarms are only generated when the alarm zone is set.	
Safety/FR/6.63	Shall be able to configure the time schedule for each alarm zone – different start and end times for each day and multiple time periods per day.	
Safety/FR/6.64	Users shall be able to define specific dates and times within time schedules so that exceptions for holidays etc. can be specified.	
Safety/FR/6.65	Shall enable the same time schedule to be applied to multiple zones.	
Safety/FR/6.66	Shall have the option of restoring the previous view after an alarm has been cleared.	
Safety/FR/6.67	Users shall be able to manually set and unset zones.	
Safety/FR/6.68	Users shall be able isolate faulty alarm inputs (detectors) such that they do not cause false alarms. Users shall be able to easily identify which alarm inputs are isolated and the reason for isolation.	
Safety/FR/6.69	Shall enable detectors to be isolated and restored on an event.	
Safety/FR/6.70	Users shall be able to specify a priority for each alarm zone (1-10)	
Safety/FR/6.71	Users shall be able to configure the alarm sound for all alarm zones in a site or for each alarm zone individually. Sound can be from any .wav file and can be sounded once or repeated while the alarm is active.	
Safety/FR/6.72	Shall allow alarms to be configured to require text from a user at the point of acknowledging and at the point of clearing.	
Safety/FR/6.73	Shall allow an alarm procedure document (.html, text or URL) to be associated with a site or to an individual alarm zone. This procedure document shall be displayed when an alarm happens.	
Safety/FR/6.74	Users shall be able to configure the actions that should be performed when an alarm occurs: • Show video from camera, camera view or salvo in specified monitors. • Stop video when alarm cleared. • Move camera to preset position. • Send email to multiple recipients, with option to include snapshots. • Perform a relay action automatically. • Start recording one or more camera – records for specified duration. • Auto-protect recording from a specified duration before the alarm.	
Safety/FR/6.75	Users shall be able to configure a second authorizing user for alarm clearing and relay actions – second user has to enter a password to authorize these functions.	
Safety/FR/6.76	Shall support the following for 3rd Party cameras through native protocols and / or ONVIF: • Motion detection events • Record on motion • Video loss • Network loss • Change video quality on event, including frame rate, resolution and bitrate	
Safety/FR/6.77	Users shall be able to configure an unlimited number of alarm groups each containing a set of alarm zones and/or detectors.	
Safety/FR/6.78	For each user or user group, it shall be possible to associate one or more video panes with each alarm group. This should also include analog monitors.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.79	Users shall be able to choose a display mode for alarm video. As multiple alarms come in, the video can either be “cascaded” across the chosen viewing panes or “queued” behind the chosen viewing panes. As alarms are cleared, the associated video is cleared from the chosen viewing panes. Cascaded video can either remain in the same video pane until cleared, or can move to the first available pane as earlier alarms are cleared.	
Safety/FR/6.80	When all alarm video is cleared from a viewing pane Shall display video and layout being viewed before any alarm was displayed.	
Safety/FR/6.81	Shall clearly mark black screen monitoring viewing windows as being distinct from normal live view windows through background colour and icon.	
Safety/FR/6.82	Shall remove any black screen monitoring analog monitors from the normal site hierarchy.	
Safety/FR/6.83	Shall have permissions to determine which users or user groups get access to which alarm groups and which windows are used to display alarm video.	
Safety/FR/6.84	Users shall be able to configure any of the available viewing panes or analog monitors as a spot monitor for viewing significant live footage.	
Safety/FR/6.85	Shall provide a toolbar option on all live viewing panes to copy the current video stream into the spot monitor.	
Safety/FR/6.86	Shall keep an audit record of what video was started and stopped in the spot monitor, by which user and what times.	
Safety/FR/6.87	Shall allow the video sequence that was viewed in the spot monitor by a selected user in a selected time period to be exported as a single incident.	
Safety/FR/6.88	Users shall be able to review all video watched by a selected user in a selected time period in an incident player. The video should be played back as one sequence in a single video pane.	
Safety/FR/6.89	Shall generate an alarm if any of the detectors within an alarm zone are activated.	
Safety/FR/6.90	Shall not generate new alarms for subsequent detector activations within the same zone so that the user only has one alarm to handle.	
Safety/FR/6.91	Shall alert new alarms with flashing icon and optionally a sound.	
Safety/FR/6.92	Shall automatically perform the actions configured for the alarm zone or detector: • Show video from camera, camera view or salvo in specified video panes or monitors • Move camera to preset position • Stop video when alarm cleared • Send email to multiple recipients • Perform a relay action • Start recording one or more cameras • Auto-protect recording from a specified duration before the alarm.	
Safety/FR/6.93	When an alarm happens, Shall be able to show live video from a camera on one pane and beside it show a looped replay from just before the alarm to just after.	
Safety/FR/6.94	From a looped replay, users shall be able to quickly jump to continuous replay from the alarm time.	
Safety/FR/6.95	The users shall be able to display a map showing the location of the alarm.	
Safety/FR/6.96	Users shall be able to view pending alarms in a list ordered by priority and time	
Safety/FR/6.97	Users shall be able to filter the alarm list to show alarms only from specific areas (sites and zones).	
Safety/FR/6.98	Shall be able to display alarm procedure document for the alarm.	
Safety/FR/6.99	Shall allow users to acknowledge alarms, entering alarm response text as required.	
Safety/FR/6.100	Shall allow users to edit the alarm response text at any time before the alarm is cleared.	
Safety/FR/6.101	Shall allow users to clear alarms, entering alarm response text as required.	
Safety/FR/6.102	Users shall be able to find historical alarms matching specified criteria: • Alarm type • Alarm state (new, acknowledged, cleared) • From site(s) • From alarm zones(s) • User(s) who acknowledged or cleared • Time range	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.103	Shall be able to escalate alarms to other user groups if the alarm is not acknowledged within a pre-defined time period.	
Safety/FR/6.104	Shall be able to escalate alarms to other user groups if the alarm is not cleared within a pre-defined time period.	
Safety/FR/6.105	Shall support different escalation time periods for different alarm priorities.	
Safety/FR/6.106	Shall be able to propagate an alarm to other areas (zones) if the alarm is not acknowledged within a pre-defined time period.	
Safety/FR/6.107	Users shall be able to produce reports of historical alarms and events and export to RTF or CSV formats	
Safety/FR/6.108	Users shall be able to authorize an alarm to be cleared, by a second user entering a password.	
Safety/FR/6.109	Users shall be able to view live or recorded video associated with the alarm.	
Safety/FR/6.110	Shall ensure that alarms are held on an alarm server, not on a user's PC.	
Safety/FR/6.111	Shall support integration with external data sources. An external Data Source shall be defined as any text string.	
Safety/FR/6.112	Shall support up to 1 external data record every second and min 2 million data records.	
Safety/FR/6.113	Shall support the ability to search and filter data records using the following: • A partial text string to search data record • Source IP address of data • Name of Data source	
Safety/FR/6.114	Shall allow for the association of data records with video data.	
Safety/FR/6.115	Integration shall be available via a freely available open interface. The interface shall be via a software development kit.	
Safety/FR/6.116	Users shall be able to configure relay actions using binary outputs on IP Cameras, encoders and decoders.	
Safety/FR/6.117	Users shall be able to configure relay actions using external outputs to 3rd party systems.	
Safety/FR/6.118	The relay activation shall be pulsed with a configurable pulse time period.	
Safety/FR/6.119	Shall support latched relay outputs.	
Safety/FR/6.120	Users shall be able to associate relay actions with specific cameras so that the actions are readily available when video is displayed from that camera.	
Safety/FR/6.121	Shall perform relay actions on alarm and event.	
Safety/FR/6.122	Shall be able to perform relay actions on a time-schedule.	
Safety/FR/6.123	Shall automatically check for devices not on the network and notify users when not available.	
Safety/FR/6.124	Shall be possible to define the users who get notified if devices become unavailable.	
Safety/FR/6.125	Users shall be able to manage the bandwidth used for network scans by configuration of: • Monitor period (minutes) • Minimum check interval (m.sec) • Perform fast check on log in • Perform fast check on refresh	
Safety/FR/6.126	Shall scan for devices using any combination of IP broadcast addresses, individual IP addresses or ranges of IP addresses.	
Safety/FR/6.127	Users shall be able to turn off scanning of devices.	
Safety/FR/6.128	Shall be able to browse on thick and thin client.	
Safety/FR/6.129	Ability to auto refresh any diagnostics view.	
Safety/FR/6.130	Shall notify users when device times are not synchronized with the viewing PC (more than 60 seconds out).	
Safety/FR/6.131	Shall notify users of problems with NVRs. The notifications will be those supported by each NVR.	
Safety/FR/6.132	Users shall be able to view the current status of an NVR with visual indicators showing whether each item is OK or indicates problems: • Total disk space • Minimum free disk space • Used disk space (total – free) • Percentage space used (used disk space / total disk space)	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• License expiry date • Maximum streams • Maximum third party streams • Number of cameras recording • Number of cameras not recording • Number of recordings • Age of last deleted recording (indicates storage being achieved for each camera) • NVR time • Any additional features supported by the NVR	
Safety/FR/6.133	Users shall be able to view per camera disk utilization for an NVR. Display a list of cameras being recorded by an NVR, showing the cameras with the highest disk usage at the top. Display the following info. For each camera: • Start time of first recording • End time of last recording • Total size of all recording • Total duration of all recordings • Recording rate (total size / total duration), in kbps	
Safety/FR/6.134	Shall provide a support information tool, which gathers together log files and site database into a zip file.	
Safety/FR/6.135	Users shall be able to configure named user groups. A group can be granted administrator rights: • Full (can configure everything) • Restricted (can configure everything except users and groups) • No configuration rights (limited user functions only)	
Safety/FR/6.136	Shall be able to hide administration options from normal users. The user interface shall be cleanly split into administrative functions and operational functions. Users who do not have administrative rights shall get a much simpler interface so that they are not confused by visible but disabled features.	
Safety/FR/6.137	Users shall be able to configure named user accounts and allocate them to user groups.	
Safety/FR/6.138	Users shall be able to enable and disable user accounts.	
Safety/FR/6.139	Users shall be able to set-up a user to use either machine OS standard authentication or a password when he logs into the Video Management System.	
Safety/FR/6.140	Users shall be able to limit the total number of video streams (live or recorded) that a user or member of a user group can display at once.	
Safety/FR/6.141	Users shall be able to limit the number of time-based thumbnail images that a user or member of a user group will display at once.	
Safety/FR/6.142	Users shall be able to allocate each user group or user a priority that is used when controlling PTZ cameras.	
Safety/FR/6.143	Users shall be able to grant global permissions to user groups or users (global permissions do not apply to specific objects such as cameras): • PTZ hold (allows a user to keep control of a PTZ camera when not moving it). • Video lockout (allows a user to perform a video lockout on any site of camera).	
Safety/FR/6.144	Users shall be able to reset access permissions on individual objects to use the access permissions of their parent site.	
Safety/FR/6.145	Users shall be able to configure application settings specific to each PC, including: • Enable or disable scheduled tasks • Enable or disable the application as the topmost window • Location for snapshot images • Format of snapshot image (bitmap or JPEG) • Folder for snapshot image • Replay incident in live or Playback view • Use software or hardware assisted video renderer • Use de-interlace filtering on live view by default • Use de-interlace filtering on playback by default	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• Set video de-interlacing • Enable or disable use of a CCTV keyboard • Serial port for CCTV keyboard • CCTV keyboard type • Video pane text scale factor (% of the default text size) • Resize text on video panes in proportion to video pane size • Video pane icon size (normal, medium, large) • Select icon size on video panes in proportion to video pane size • Date / time display on video panes (none, all, selected) • Load bookmarks on startup • Spot monitor (external monitor or specified video pane) • Protect recordings by default when exporting • Write date and time on exported recordings	
Safety/FR/6.146	User should be able to extract reports on demand.	
Safety/FR/6.147	Users shall be able to prevent simultaneous listen and speak (full duplex audio).	
Safety/FR/6.148	Users shall be able to configure the use of buffered playback when reviewing recordings.	
Safety/FR/6.149	Users shall be able to enable or disable alert messages.	
Safety/FR/6.150	Users shall be able to log into the Video Management System manually.	
Safety/FR/6.151	It shall be possible to start the Video Management System from the command line with the following options: • Username and password. • Normal, full screen or video-only modes. • Site database.	
Safety/FR/6.152	Shall allow users to log out and log in without closing the application.	
Safety/FR/6.153	Shall have an option to require all users to re-enter their password when logging out.	
Safety/FR/6.154	Shall remember display settings on a PC for each user at log off and restore settings at log in: • Which cameras are displayed in which video panes. • PTZ controls displayed. • Map window position. • Alarm window position. • Video window positions (default hidden). • Main window size and position and site explorer width. • Recording calendar displayed.	
Safety/FR/6.155	Users shall be able to change their own password (if given write permission to the site database).	
Safety/FR/6.156	Users shall be able to change their default location on the tree hierarchy.	
Safety/FR/6.157	Users shall be able to lockout all other users preventing them from viewing or recording video from a selected camera or all cameras in a selected site.	
Safety/FR/6.158	Shall support an audit trail that can log user actions to an industry standard databases as open source.	
Safety/FR/6.159	Users shall be able to specify the authentication method to be used between the client application and the audit trail database: • Local user password. • Operating System user password.	
Safety/FR/6.160	The audit trail shall log the following user actions to the audit trail database: • User logged on. • User attempted to log on and was denied access. • User logged off. • User changed "home" site. • User acknowledged an alarm. • User cleared an alarm. • User received an alert message (e.g. device not available). • User starting playing back a recording (forward). • User started playing back a recording (backwards).	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
	• User stopped playing back a recording. • User denied playing back a recording or playback failed. • User took control of a PTZ camera. • User released control of a PTZ camera. • Second user authorized relay action. • Second user authorized alarm to be cleared. • Second user denied authorizing a relay or alarm to be cleared. • Export recordings. • Protect recordings. • Manual start or stop recording. • User log out denied. • User starts playing live video from a specific camera. • User stops playing live video from a specific camera. • Creation, deletion or editing items stored in the Video Management System configuration database. • User created a bookmark.	
Safety/FR/6.161	The audit trail shall log the following information for each entry in the audit log: • Name of the user performing the action. • DNS name of computer running in ICCC. • The name of the application writing to the log. • A string naming the type of action performed e.g. Log on. • Name and matrix number of the object that the action applies to e.g. camera name and number. • Further information about the action, in a structured form. • Severity (applies to error message received log entry).	
Safety/FR/6.162	The user shall be able to export a report from the audit trail database into a standard reporting tool, e.g. MS Excel.	
Safety/FR/6.163	Shall discover IP Video devices on a network either by broadcast address or unicast addresses for each device.	
Safety/FR/6.164	Shall allow configuration of IP Video System devices via their web configuration interface.	
Safety/FR/6.165	Shall enable mass configuration of devices, in particular encoder settings on IP cameras and encoders.	
Safety/FR/6.166	Administrators shall be able to view video from each stream at the same time as making changes to the media parameters on an encoder to aid configuration.	
Safety/FR/6.167	Administrators shall be able to upgrade the firmware on IP Video System devices - multiple devices can be upgraded in one go.	
Safety/FR/6.168	Administrators shall be able to create a hierarchy of sites and sub-sites for organizing cameras and other items by location.	
Safety/FR/6.169	Administrators shall be able to set the time-zone on a site - different sites can each have their own time zone.	
Safety/FR/6.170	Users shall be able to reorder sites under their parent site (sites are ordered by number).	
Safety/FR/6.171	Shall be able to automatically create a site hierarchy within a site database containing IP Video System devices visible on the network.	
Safety/FR/6.172	Users shall be able to create sequences and salvos within the sites, set up 24/7 recording for each camera and enable video loss and network loss alarms.	
Safety/FR/6.173	Users shall be able to add cameras, monitors, alarm panels, alarm servers and NVRs to sites by dragging and dropping, selecting from a list or manually entering the IP Address and name.	
Safety/FR/6.174	Users shall be able to remove devices from sites.	
Safety/FR/6.175	Users shall be able to move devices, and other items such as sequences, salvos, and sub sites from one site to another by dragging and dropping.	
Safety/FR/6.176	Users shall be able to enter a localized display name for cameras, monitors, alarm panels, alarm servers and NVRs which overrides the name stored on the device.	
Safety/FR/6.177	Shall enable a copy of the configuration database to be cached locally on each user workstation to ensure continuity of operation when a connection to the central database is not available.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.178	Shall support a configuration database that is divided into multiple 'segments', e.g. one segment for each site. Shall allow each segment to be configured and accessed independently.	
Safety/FR/6.179	Shall support user access permissions so that only authorized users can access specific segments.	
Safety/FR/6.180	When the configuration database is divided into segments, Shall allow all sites to monitored e.g. from a central monitoring facility.	
Safety/FR/6.181	Users shall be able to create one or more maps for each site by importing an image for the background. The following image formats shall be supported: • Bitmap (BMP) • JPEG (JPG) • Portable Network Graphics (PNG) • AutoCAD drawings (DWG) • GIS	
Safety/FR/6.182	Users shall be able to add links to other maps.	
Safety/FR/6.183	Users shall be able to reposition items by drag and drop or entering specific coordinates.	
Safety/FR/6.184	Users shall be able to add cameras to map via drag and drop.	
Safety/FR/6.185	Users shall be able to specify the field of view for each camera.	
Safety/FR/6.186	Users shall be able to add alarm zones and detectors to map.	
Safety/FR/6.187	For alarm zones, users shall be able to have options to not display the alarm icon and/or name unless the alarm is active.	
Safety/FR/6.188	For zones and detectors, users should be able to configure a detector/zone area on the map.	
Safety/FR/6.189	Users shall be able to specify the amount of detail displayed for each object including icons, matrix numbers and labels.	
Safety/FR/6.190	Colour schemes shall be configurable to make text and fields-of-view more visible.	
Safety/FR/6.191	The map shall be fully scalable with zoom and pan supported under mouse control.	
Safety/FR/6.192	Users shall be able to displays the previous maps viewed (back, forward).	
Safety/FR/6.193	Users shall be able to link to any map from any map.	
Safety/FR/6.194	Users shall have the option of scaling icons to a fixed zoom level.	
Safety/FR/6.195	The map should be viewable on a separate monitor from the main video(s).	
Safety/FR/6.196	Users shall be able to display live and recorded video from any camera on a map (drag and drop).	
Safety/FR/6.197	Users shall be able to view video from some or all of the cameras on a map via drag-select.	
Safety/FR/6.198	Users should be able to click on the field-of-view of any camera to view the video.	
Safety/FR/6.199	Where fields-of-view overlap, clicking on the convergent area should result in all cameras being displayed.	
Safety/FR/6.200	Activated alarms shall be visually represented on the map.	
Safety/FR/6.201	Where detector/zones areas have been configured, these should be visually represented as being in an alarmed state.	
Safety/FR/6.202	Where detector/zones areas have been configured and in an alarmed state, the user should be able to start video from all cameras associated with that zone by clicking on it.	
Safety/FR/6.203	Users shall be able to: • Manage alarms from a map • Clear alarms • Acknowledge alarms • View Video associated with an alarm • Isolate/restore alarms • Set/unset detectors	
Safety/FR/6.204	Users shall be able to trigger events to binary outputs on cameras or encoders.	
Safety/FR/6.205	Shall include a restricted access version of the video viewing and replay application that prevents all users from accessing the setup screens even if they have an administrator login.	
Safety/FR/6.206	Shall provide a restricted access site database management utility, which prevents creation of new site databases.	

S.No	Minimum Functional Requirement	Compliant (Yes/ No)
Safety/FR/6.207	Shall provide a restricted access version of the video viewing and replay application, which prevents all users from modifying the audit log configuration even if they have an administrator login.	
Safety/FR/6.208	The Video Management System • Should have Mobile device/Tablet device client software (Supporting Android, iOS and Windows Mobile/Surface). • Mobile client should be controlled and configured through central software, capable of live streaming the video from mobile client to Video Management System. • Mobile client should provide UI over mobile to view cameras deployed across city, select particular camera and view the live video stream. • Mobile client should provide role based access that can be configured for users to view and control particular cameras. • Should be able to support Min 10 mobile clients and 15 Tablets without additional cost and scalable up to 500.	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements		Compliant (Yes / No)
1. PTZ Camera			
	Parameter	**Minimum Requirement**	
Safety/TR/1.01	Video Compression	H.264, H.265/MJPEG/ MPEG-4 or better	
Safety/TR/1.02	Video Resolution	1920 X 1080	
Safety/TR/1.03	Frame rate	Min 30 fps or better	
Safety/TR/1.04	Image Sensor	1/3" OR ¼" or better Progressive Scan CMOS	
Safety/TR/1.05	Lens	Auto-focus, 4.3 - 129 mm (corresponding to 30x)	
Safety/TR/1.06	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)	
Safety/TR/1.07	Day/Night Mode	Colour, Mono, Auto	
Safety/TR/1.08	S/N Ratio	≥ 50Db	
Safety/TR/1.09	PTZ	Pan: 360°	
		endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual)	
		Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual)	
		30x optical zoom and 10x digital zoom	
		64 preset positions Auto-Tracking	
		Pre-set tour	
Safety/TR/1.10	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range	
Safety/TR/1.11	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6	
Safety/TR/1.12	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption	
Safety/TR/1.13	Operating conditions	As per City requirement	
Safety/TR/1.14	Casing	NEMA 4X / IP-66 rated	
Safety/TR/1.15	Certification	UL/EN,CE,FCC	
Safety/TR/1.16	Local storage	Minimum 64 GB Memory card in a Memory card slot	
Safety/TR/1.17	IR Cut Filter	Automatically removable IR cut-filter	
Safety/TR/1.18	IR	Internal/External. IR range should be 100 meter or better	

2. Fixed Camera			
Safety/TR/2.01	Video Compression	H.264, H.265/MJPEG/ MPEG-4 or better	
Safety/TR/2.02	Video Resolution	1920 X 1080	
Safety/TR/2.03	Frame rate	Min. 30 fps or better	
Safety/TR/2.04	Image Sensor	1/3” Progressive Scan or better CMOS	
Safety/TR/2.05	Lens Type	Varifocal, C/CS Mount, IR corrected full HD	
Safety/TR/2.06	Lens	Auto IRIS - 8 – 50 mm, F1.4	
Safety/TR/2.07	Minimum Illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE)	
Safety/TR/2.08	IR Cut Filter	Automatically Removable IR-cut filter	
Safety/TR/2.09	Day/Night Mode	Colour, Mono, Auto	
Safety/TR/2.10	S/N Ratio	≥ 50Db	
Safety/TR/2.11	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Wide Dynamic Range	
Safety/TR/2.13	Audio	Audio Capture Capability	
Safety/TR/2.14	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, QoS, IPV4, IPV6	
Safety/TR/2.15	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption	
Safety/TR/2.16	Operating conditions	As per City requirement	
Safety/TR/2.17	Casing	NEMA 4X / IP-66 rated	
Safety/TR/2.18	Certification	UL/EN,CE,FCC	
Safety/TR/2.19	Local storage	Minimum 64 GB Memory card in a Memory card slot	
Safety/TR/2.20	IR	Internal/External. IR range should be 100 meter or better	
Safety/TR/2.21	Field of View	Shall have at least 70 degrees field of view (horizontal)	
Safety/TR/2.22	Intelligent Video	Motion detection and tampering alert	
Safety/TR/2.23	Alarm I/O	Minimum 1 input and 1 output contact for 3rd part interface	
3. Infrared Illuminators			
Safety/TR/3.01	Range	Min. 100 meters, with adjustable angle to cover the complete field of view at specified locations	
Safety/TR/3.02	Minimum Illumination	High sensitivity at Zero Lux	
Safety/TR/3.03	Power	Automatic on/off operation	
Safety/TR/3.04	Casing	NEMA 4X / IP-66 rated	
Safety/TR/3.05	Operating conditions	As per City requirement	
Safety/TR/3.06	Certificate	CE, FCC, UL/EN	
Safety/TR/3.07	Range	Min. 100 meters, with adjustable angle to cover the complete field of view at specified locations	
Safety/TR/3.08	Minimum Illumination	High sensitivity at Zero Lux	
Safety/TR/3.09	Power	Automatic on/off operation	
4. Network Video Recorder (NVR)			
Safety/TR/4.01	The Network Video Recorder (NVR) will be connected via a Gigabit Ethernet network		
Safety/TR/4.02	NVR shall be of N+N configuration with RAID 6 configuration		
Safety/TR/4.03	All equipment shall be designed to provide a usable life of not less than 15 years		
Safety/TR/4.04	The NVRs shall have a self-diagnostic feature including disk status, CPU usage, motherboard temperature, network status and fan status		

Safety/TR/4.05	The NVRs shall be support interface using 10/100/1000BaseTX. It shall support a total throughput of at least 700 Mbps	
Safety/TR/4.06	The NVR shall be powered using minimum power	
Safety/TR/4.07	Each NVR unit shall be maximum of 2U height	
Safety/TR/4.08	The NVR shall support both Linux and Windows platform	
Safety/TR/4.09	The NVR shall be capable of digitally signing stored video and digitally sign exported video to ensure chain of trust	
Safety/TR/4.10	The NVR shall have failover and redundancy built in with seamless playback without manual intervention	
Safety/TR/4.11	The NVR shall support a minimum of 200 recorded video streams and 20 playback streams with minimum playback of 400 Mbps	
Safety/TR/4.12	All equipment shall be modularly upgradeable so that it does not need to be replaced in its entirety to increase memory capacity, to upgrade processing performance, or to reconfigure I/O options	
Safety/TR/4.13	Normal state (non-alarm) recording configuration to provide for “Detection” as defined by ULC-317-1997 and as follows: • Resolution HD • Normal Frame rate of 25 FPS	
Safety/TR/4.14	Alarm state recording configuration to provide for “Recognition” as defined by ULC-317-1997 and as follows: • Resolution of HD • Frame rate of 25 FPS • Alarm state recording of one track of audio at 32 Kbit	
5. Central Application		
Safety/TR/5.01	The software shall be able to run on any PC based on industry standard OS	
Safety/TR/5.02	The software shall support ONVIF compliant cameras and devices	
Safety/TR/5.03	The software shall show live video from IP Cameras and Video Transmitters in MJPEG, MPEG4 and H.264, H.265 formats or better	
Safety/TR/5.04	The software shall support cameras with resolutions ranging from Standard Definition, High Definition (HD) and up to 5 Megapixel	
Safety/TR/5.05	The software shall show video across 4 displays per workstation - each display can have up to 25 viewing panes	
Safety/TR/5.06	The software shall allow configuration of the video and audio stream settings for each user, depending on the support hardware	
Safety/TR/5.07	Users shall be able to change the video pane layout in each of the 4 screens independently: • Grid layouts: 1x1, 2x2, 3x3, 4x4, 5x5 • Widescreen layouts: 2x3, 3x4, 4x6 • Hotspot layouts based on 3x3, 4x3, 4x4, 5x5 larger pane in top, left • Hotspot layouts based on 4x3, 4x4, 5x5 larger panes in center	
Safety/TR/5.08	Users shall be able to change the aspect ratio in each of the 4 video windows independently in order to display Standard Definition or High Definition video. Choose between: • Widescreen (16:9) • Standard (4:3)	
Safety/TR/5.09	Users shall be able to move any image from one display screen to another via drag-and-drop	
Safety/TR/5.10	Users shall be able to digitally zoom up to 1000% and also digitally scroll live video from any camera using the mouse wheel	
Safety/TR/5.11	The software shall allow the removal of interlacing artefacts from 4SIF video using the following criteria: • Best performance • Best image quality • Smoothest rendering	
Safety/TR/5.12	The software shall allow the display of objects detected via analytics on the video (up to 10 at once)	
Safety/TR/5.13	Users shall be able to view stream statistics on all current video streams, including the following information: • Frame rate • Resolution (SIF, 2SIF, 4SIF,720p, 1080p, 5MP)	

	• Current bit-rate • Audio bit-rate	
6. Poles for Cameras		
Safety/TR/6.01	Shall be minimum 20ft (6.5mts) height as per NHAI norms	
Safety/TR/6.02	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate size 30x30x15 cm. suitable for wind speed 50m/sec with suitable arm bracket and with J type foundation bolts . Fabrication in accordance with IS 2713 (1980)	
Safety/TR/6.03	The pole would be fixed on an adequate and strong foundation so as to withstand city weather conditions and wind speed of 150km / hr	
Safety/TR/6.04	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100cms or better	
Safety/TR/6.05	Lighting arrestors with proper grounding	
Safety/TR/6.06	Sign board depicting the area under surveillance and with the serial number of the pole	
Safety/TR/6.07	The height of the pole shall be as per requirement of the location varying from 6.Mts to 12/15 Mts.	

7. Online UPS for Field Locations

S.No	Parameter	Minimum Technical Requirement	Compliant (Yes/ No)
Safety/TR/7.01	Capacity	Adequate capacity to cover all above IT Components at respective field locations.	
Safety/TR/7.02	Technology	IGBT based PWM Technology, True Online UPS	
Safety/TR/7.03	Input Frequency Range	45 to 55 Hz	
Safety/TR/7.04	Output Frequency Range	45 to 55 Hz	
Safety/TR/7.05 Safety/TR/7.06	Output Voltage	220VAC - 230VAC	
Safety/TR/7.07	Voltage Regulation	+/-2% (or better) and with built- in Over Voltage Cut off facility in the Device	
Safety/TR/7.08	Frequency	50 Hz +/- 0.1% (free Run Mode)	
Safety/TR/7.09	Harmonic Distortion (THD)	< 3% (linear load)	
Safety/TR/7.10	Output Waveform	Pure Sine wave	
Safety/TR/7.11	Output Power Factor	0.8 or more	
Safety/TR/7.12	Battery Backup	Adequate and required battery backup to achieve required uptime of field device as well as SLA of the overall solution.	
Safety/TR/7.13	Battery Type	Lead acid, Sealed Maintenance.	
Safety/TR/7.14	General Operating Temperature	As per City condition and requirement.	
Safety/TR/7.15	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection	
Safety/TR/7.16	Bypass	Automatic, Manual Bypass Switch.	
Safety/TR/7.17	Certifications	For Safety & EMC as per international standard.	
Safety/TR/7.18	Overall Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake.	

Other Smart Elements:

Public Address System (PAS) and Variable Message Signboards (VaMS)

Objective

Traffic Information Dissemination System comprising key components namely, Variable Message Signboard (VaMS)/ Dynamic Message Sign (DMS) and Public Address (PA) system aims to provide real-time information on (a) prevailing traffic conditions on the road and (b) emergencies, if any, on account of traffic accidents to enable the key stakeholders, including traffic police, commuters/ road users to take informed and timely decisions.

The envisaged benefits of VaMS / PAS are as follows:

- Variable Message Signboard (VaMS) enables dissemination of standard / customized / dynamic mode of information/ messages/ alerts related to the traffic conditions on the road based on information received from the Integrated Command and Control centre (ICCC) to help key stakeholders including traffic police, commuters/ road users to take informed decisions
- Public Address (PA) system enables key stakeholders including Traffic Police to announce real-time advisories/ information to the road users/ commuters and general public on prevailing traffic conditions and emergency, if any, based on information from ICCC.
- The system integrates with the Traffic Management & Emergency Response Management System for making automated, system generated, or manual announcements.

Scope of Work

The broad scope of work to be covered under this sub module shall include the following, but is not limited to:

- The MSI shall install IP based VaMS boards on approximate 13 locations across city of Rourkela. VaMS board displays are to be controlled by Rourkela Traffic Police personnel from the ICCC. The purpose of the VaMS boards is to provide the commuters with information about traffic/congestion conditions and alternate routes/diversions in case of high traffic on roads.
- The MSI, in consultation with Rourkela Police can propose alternate locations apart from the locations mentioned in this RFP for installing the VaMS boards where their effectiveness in communicating information about traffic conditions in Rourkela shall be maximized.
- Rourkela Police shall review and approve the proposed locations. The MSI shall install the VaMS boards on the approved locations.

List of 29 traffic junctions for installation of PAS, as provided in the table below:

S.No.	Junction Name	Type of Junction (No. of Arms)
1	Birsa Chowk	6
2	Traffic tower	3
3	Sector-2	4
4	Ambagan Chowk	4
5	7/17 Chowk	4
6	7/15 Chowk	4
7	Sector-8	4
8	DPS Chowk	4
9	Air strip Chowk	3
10	SOS Village Chowk	3
11	Chhend Chowk	3

S.No.	Junction Name	Type of Junction (No. of Arms)
12	DAV Chowk	4
13	Gadiatola Chowk	4
14	Municipality Chowk	3
15	Sarna Chowk	3
16	Bania Chowk	4
17	Traffic gate	4
18	Madhusudan Chowk	4
19	Hockey Chowk	3
20	Panposh Chowk	4
21	Shani Mandir	3
22	Hi-tech Medical Chowk	3
23	Civil Township parking Chowk	3
24	Dandiapadi Chowk	3
25	Vedvyas Chowk	3
26	Rangila Chowk	4
27	Chhend BSNL Chowk	4
28	Diesel Colony Chowk	3
29	Chowdhary Petrol Pump	3

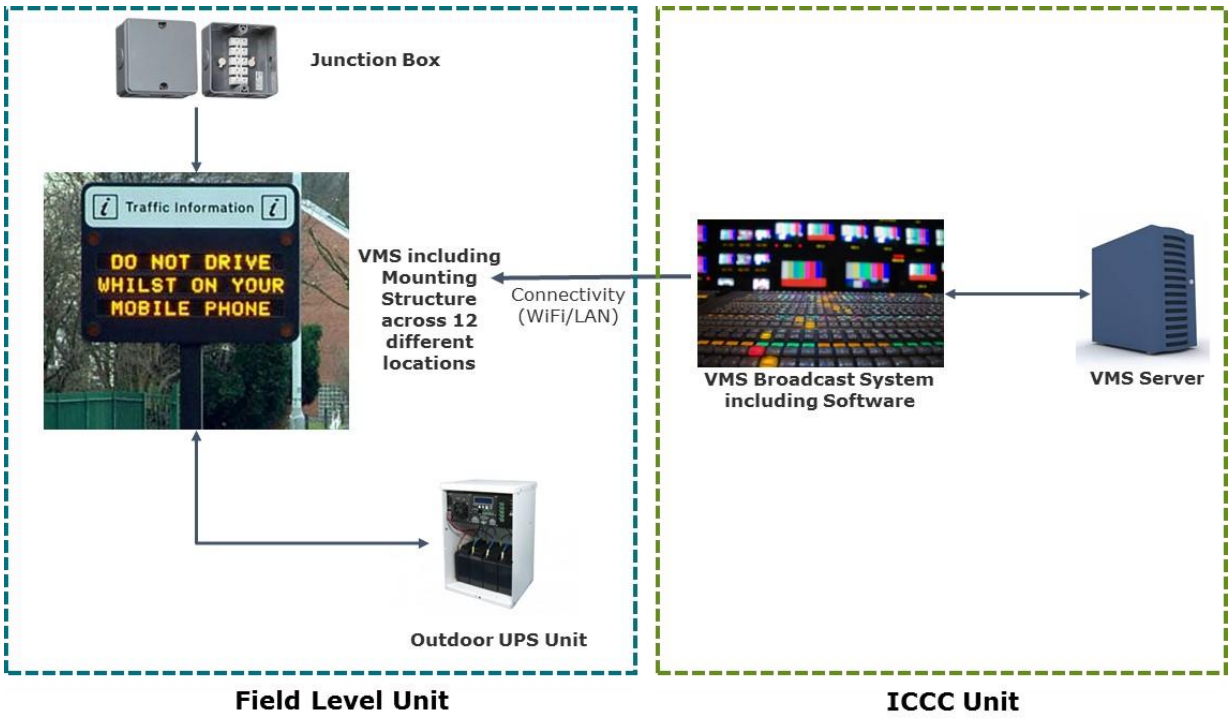
VaMS

List of 13 locations for installation of VaMS, provided in the table below:

S.No.	Location
1.	Bisra Chowk
2.	Sector -2
3.	Ambagan Chowk
4.	Municipality chowk
5.	Traffic Gate Chowk
6.	Ambedkar Chowk
7.	Chhend Chowk
8.	Hockey Chowk
9.	Panposh Chowk
10.	Vedvyas Chowk
11.	Sector 19 IGH Chowk
12.	Koel Club Chowk
13.	Daily Market

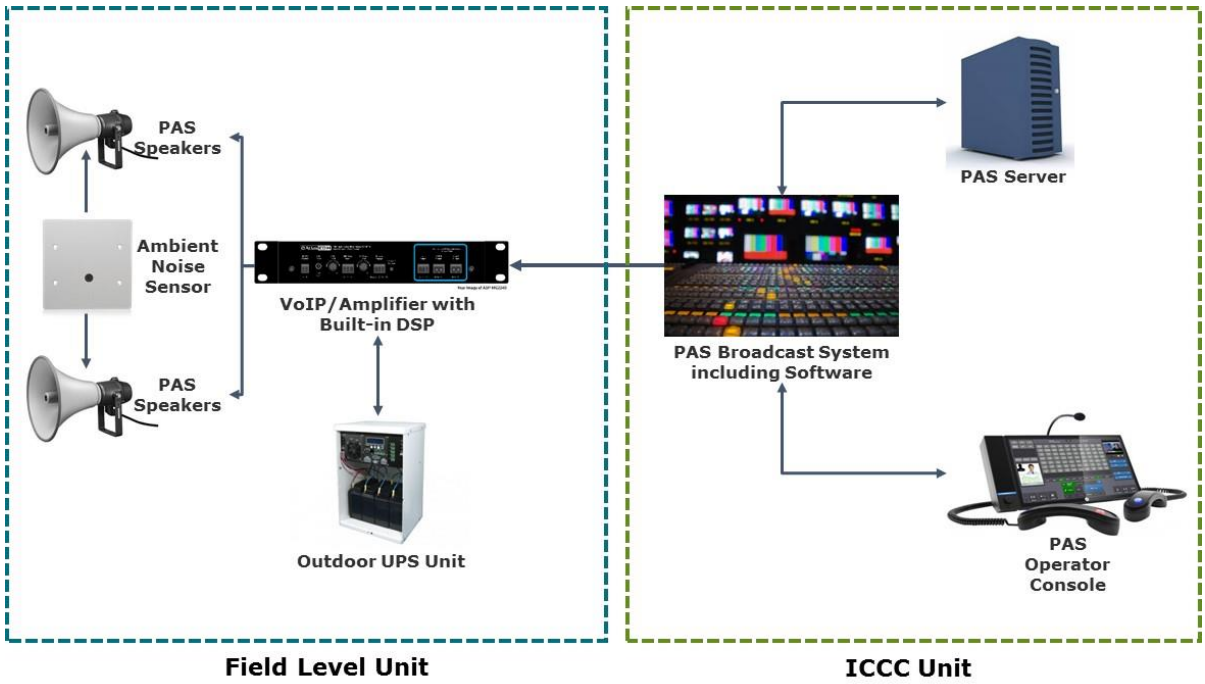
Indicative Solution Architecture

A high level schematic diagram for the proposed Variable Message Signboard to enable the key stakeholders, including the Traffic police and the citizens to take informed and timely decision based on the prevailing traffic conditions in the city.is presented below:



Solution Architecture for Variable Message Signboards

An indicative solution architecture for the proposed Public Address system to provide real-time information to the citizens on (a) prevailing traffic conditions on the road and (b) emergencies, if any, on account of traffic accidents is presented below:



Solution Architecture for Public Address System

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. Variable Message Signboards (VaMS)		
VaMS/FR/1.01	VaMS solution shall be able to display real-time as well as static data.	
VaMS/FR/1.02	VaMS solution shall be a fully customizable solution for each display/ location to show live traffic-related information, live congestion related information specific to that location/ corridor.	
VaMS/FR/1.03	VaMS solution shall be able to provide automatic real-time information like weather updates, alternate route options useful to the road user.	
VaMS/FR/1.04	VaMS Solution shall have the capability to be integrated with disaster management & emergency response data sources to provide instant alerts to road users & public.	
VaMS/FR/1.05	SMART VaMS solution shall allow integration with Speed Radars/lasers for speed monitoring and Driver feedback applications to reduce accident on roads.	
VaMS/FR/1.06	SMART VaMS solution shall allow distribution of emergency messages to specific individual / group or all VaMS boards via secured Mobile/ Tablet application.	
VaMS/FR/1.07	SMART VaMS solution shall be capable of reading live data from road side sensors. Example: - Parking, Air Quality etc.	
VaMS/FR/1.08	If there is no data connectivity due to network issues on the thin client then the VaMS shall display the last uploaded content / programmed content, thus ensuring uninterrupted performance.	
VaMS/FR/1.09	The system should be easy to manage and operate from a single control room and the central control software is capable of managing at least 500 boards.	
VaMS/FR/1.10	In the event of central server failure, each of the SMART VaMS boards should be individually capable of continuous & uninterrupted display of real time traffic & other information as per last configuration thereby ensuring continuous operation.	
VaMS/FR/1.11	There shall be an option to view latest content screen shot of every display on the centrally hosted VaMS Manager Application	
VaMS/FR/1.12	Android/ Windows / iOS App shall be provided for entering Emergency messages and distributing to the VaMS Displays from the App with clear time lines (Start time & Date, End time and Date). Authentication key shall be provided to the authorized users only.	
VaMS/FR/1.13	Automated email alerts at set intervals shall be provided in case the VaMS thin clients are not connecting to the central manager application.	
VaMS/FR/1.14	The system shall maintain the history of messages archived for future reference and analysis.	
VaMS/FR/1.15	All boards shall be connected and controlled centrally via one software application and server. The software patches/upgradation should be free for 5 years post go live	
VaMS/FR/1.16	It shall be capable to integrate with any other solutions (including Intelligent Transport Solution) as and when required on availability of protocols. It should have the ability to integrate common content wherever possible.	
VaMS/FR/1.17	The intended information to be displayed shall have the feature to schedule and display data at any date and time.	
VaMS/FR/1.18	VaMS solution shall be installed at the control center and shall also be capable of providing viewing facilities as directed by the Engineer.	
VaMS/FR/1.19	VaMS shall be capable to maintain logs on the server for a period of 12 months.	
VaMS/FR/1.20	VaMS solution shall display pictograms and text message in English, Odiya, Hindi and other regional languages.	
VaMS/FR/1.21	VaMS Solution shall have the capability to define groups for displays, so that specific messages can be displayed to targeted boards.	
VaMS/FR/1.22	VaMS solution shall work in an automated fashion. No manual intervention shall be required for displaying the contextual, real-time information.	
VaMS/FR/1.23	VaMS solution can be on-premise or cloud-based solution.	
VaMS/FR/1.24	The solution should have a photo sensor that can detect the external light and adjust the display brightness accordingly.	
VaMS/FR/1.25	Each VaMS should have the GPS coordinates which should be plotted in the GIS map.	
VaMS/FR/1.26	The system should be capable to detect any unauthorized opening of the display doors at the central server location and alert the user.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
VaMS/FR/1.27	Smart VaMS software should be capable to detect the non-working status of SMPS Voltage, LED pixel with Red, Blue, Green LEDs, FRC Cables remotely and alert the user.	
VaMS/FR/1.28	Certifications: • Display should have certifications for FCC, CE, RoHS, IP65 from front side and IP55 for whole cabinet as a regulatory compliance. • Display should be CB certified • The system compliant to optical parameters of EN12966 with Beam width of B7, Luminance of L3, Luminance ratio of R3 and Color Class as C2	
VaMS/FR/1.29	VaMS shall enable RSCL/Police to communicate effectively with citizens and also improve response while dealing with exigency situations. These shall also be used to regulate the traffic situations across the city by communicating right messages at the right time.	
VaMS/FR/1.30	The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the ICCC in real time	
VaMS/FR/1.31	The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops	
VaMS/FR/1.32	The VaMS should display text and graphic messages using Light Emitting Diode (LED) arrays	
VaMS/FR/1.33	The System should be able to display failure status of any LED at ICCC	
VaMS/FR/1.34	The System should support Display characters in true type fonts and adjustable based on the Operating system requirement	
VaMS/FR/1.35	The VaMS workstation at the ICCC should communicate with the VaMS controller through the network. It should send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the VaMS workstation should receive status data from the VaMS controller	
VaMS/FR/1.36	VaMS controllers should continuously monitor the operation of the VaMS via the provided communication network	
VaMS/FR/1.37	Operating status of the variable message sign should be checked periodically from the ICCC	
VaMS/FR/1.38	It shall be capable of setting an individual VaMS or group of VaMS's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means	
VaMS/FR/1.39	It shall be capable of being programmed to display an individual message to a VaMS or a group of VaMS's at a pre-set date and time	
VaMS/FR/1.40	It shall also store information about the time log of message displayed on each VaMS. The information stored shall contain the identification number of the VaMS, content of the message, date and time at which displayed message/picture starts and ends	
VaMS/FR/1.41	The central control computer shall perform regular tests (pre-set basis) for each individual VaMS. Data communication shall be provided with sufficient security check to avoid unauthorized access	
VaMS/FR/1.42	The system shall have capability to divide VaMS screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.	
VaMS/FR/1.43	The system shall also provide airtime management and billing system for paid content management	
VaMS/FR/1.44	Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VaMS	
VaMS/FR/1.45	Capable of controlling brightness & contrast through software	
VaMS/FR/1.46	Real time log facility – log file documenting the actual sequence of display to be available at central control system	
VaMS/FR/1.47	Multilevel event log with time & date stamp	
VaMS/FR/1.48	Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log	
VaMS/FR/1.49	Location of each VaMS will be plotted on GIS Map with their functioning status which can be automatically updated	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
VaMS/FR/1.50	Report generation facility for individual/group/all VaMSs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report	
VaMS/FR/1.51	Configurable scheduler on date/day of week basis for transmitting preprogrammed message to any VaMS unit	
VaMS/FR/1.52	Various users shall access the system using single sign on and shall be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc	
VaMS/FR/1.53	Components of the architecture should provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage	
VaMS/FR/1.54	The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Antivirus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired	
VaMS/FR/1.55	Remote Monitoring a. All VaMS shall be connected/configured to Traffic Monitoring system for remote monitoring through network for two way communication between VaMS and control Room to check system failure, power failure & link breakage. b. Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED	
VaMS/FR/1.56	System shall use open standards and protocols to the extent possible	
VaMS/FR/1.57	System shall use open standards and protocols to the extent possible. Facility to export reports to excel and PDF formats	
VaMS/FR/1.58	System shall be capable of • Providing reports related to the video broadcasted across VaMS • Summary reports based on number seconds the videos played at each VaMS for goven time, day, week, month, etc.	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
2. Public Address System (PA)		
PAS/FR/2.1	The PA system shall have a voice based sub-system to disseminate information/ messages quickly to the road users/ commuters/ public particularly during emergencies.	
PAS/FR/2.2	The system should have the capability of designing the messages based on the situation or context for broadcasting through PA system.	
PAS/FR/2.3	The PA system shall have provision for emergency announcements to be made on per location, selection of locations, or a system wide basis.	
PAS/FR/2.4	The PA system shall have the ability to produce and play out either pre-recorded messages or make live announcements.	
PAS/FR/2.5	The PA system shall be integrated with the Traffic Management & Emergency Response Management System for making automated, system generated, or manual announcements.	
PAS/FR/2.6	The system shall have the ability to integrate with CCTV systems, VaMSs and other main/sub systems at ICCC for configuring and broadcasting the messages to the road users/ commuters.	
PAS/FR/2.7	The system shall have the ability to configure the messages with the static or dynamic text from various applications/systems to form a complete message as and when required.	

PAS/FR/2.8	The system shall have the capability to recognize and broadcast messages based on some analytics, including sound alerts, system alerts, incident alerts, etc.	
PAS/FR/2.9	The system shall integrate with other network PA systems or third party application systems where the alerts are generated to broadcast messages.	
PAS/FR/2.10	The system should be able to generate various statistics, reports & MIS from time to time.	
PAS/FR/2.11	The system shall be designed and installed in a manner that it minimizes community sound pollution. It shall comply with the requirements of local noise level standards & other by-laws.	
PAS/FR/2.12	The system shall have the ability to schedule category wise system messages or overall messages in advance for a specified period of time to selective or all PAS locations.	
PAS/FR/2.13	The system message quality shall be clearly audible from its location to a distance of more than 100 m without any distortion and loss in quality of the sound factoring the traffic conditions prevalent in the city.	
PAS/FR/2.14	The PA should provide the status indicators on the system at the command centre.	
PAS/FR/2.15	The PA system shall have a monitoring dashboard at the ICCC showing its schematic layout highlighting all connected nodes on GUI. If any particular node is disconnected from the control room, the same shall raise an alarm to the ICCC operator GUI & appropriate action shall be taken to rectify the same.	
PAS/FR/2.16	The monitoring dashboard shall allow the ICCC operator to click on any node and view the details of “operator” logged in, time duration since logged in, summary of operations performed, disable/enable PA system.	
PAS/FR/2.17	If ICCC operator or any other user from ICCC disable/ enable/ operate any active device remotely, the same shall be captured in ICCC activity report with all details including but not limited to date, time, device, action performed etc.	
PAS/FR/2.18	The monitoring dashboard shall show the status (connected/disconnected, faulty/working) of all logical devices (PA system) connected to a particular node when clicking on a node from the monitoring dashboard GUI.	
PAS/FR/2.19	In case of any fault in the devices connected to a node, or connectivity failure with a node, a pop-up message shall appear on the monitoring dashboard workstation.	
PAS/FR/2.20	Fault assignment to the maintenance team shall be managed and controlled by the system software. Once a fault is assigned by the ICCC operator or authorized user to the maintenance team, the same shall be displayed in the maintenance module and once fault is closed/resolved by the maintenance team it shall be updated automatically (in case of active devices) or else updated manually in the software application/maintenance module.	
PAS/FR/2.21	The access to monitoring dashboard shall be specific to the privilege of the user which can be defined in the system & shall be specific to a group/part of node locations.	

Minimum Technical Requirements

Variable Message Signboards (VaMS)

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. Full color LED display		
VaMS/TR/1.01	Minimum 3.0m length X 1.5m height X 0.2m depth. (3000mm x 1500mm X 200mm approx.)	
VaMS/TR/1.02	Colour LED: Full Colour, class designation C2 as per IRC/EN 12966 standard	
VaMS/TR/1.03	Luminance Class/Ratio: L3 as per IRC/EN 12966 standards	
VaMS/TR/1.04	Luminance Control & auto Diming	
VaMS/TR/1.05	Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software	
VaMS/TR/1.06	Auto dimming capability to adjust to ambient light level (sensor based automatic control)	
VaMS/TR/1.07	Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance	
VaMS/TR/1.08	Contrast Ratio: R3 as per IRC/EN 12966 standard	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
VaMS/TR/1.09	Beam Width: B6+ as per IRC/EN12966 standards	
VaMS/TR/1.10	Pixel Pitch: 12mm or better	
2. Picture Display		
VaMS/TR/2.1	At least 300mm as per IRC /EN 12966 standards	
VaMS/TR/2.2	Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at-least	
VaMS/TR/2.3	Synchronized Dot to Dot display	
VaMS/TR/2.4	Capable of displaying real time message generated by ICCC	
VaMS/TR/2.5	Special frontal design to avoid reflection	
VaMS/TR/2.6	Display shall be UV resistant	
VaMS/TR/2.7	Viewing Angle: B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road	
VaMS/TR/2.8	Viewing Distance: Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles	
VaMS/TR/2.9	VaMS shall have self-test diagnostic feature to test for correct operation	
VaMS/TR/2.10	Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated	
VaMS/TR/2.11	All periodic self-test results shall be relayed to the ICCC in real time to update the status of the VaMS	
3. Client Management Software		
VaMS/TR/3.01	Should be able to play the media at predefined times on all functioning days.	
VaMS/TR/3.02	No Personnel should be required to either switch on, switch off, power off, log in or log out procedures. All the above functions should function automatically as scheduled.	
VaMS/TR/3.03	Should have Multiple Screen Layouts with Multiple Independent Zones.	
VaMS/TR/3.04	Should be able to play Standard Multimedia Files: Flash, Videos, Images, etc.	
VaMS/TR/3.05	Able to play Time-Sensitive Content – able to purged the expired old content.	
VaMS/TR/3.06	user should be able to Connect on “as-and-when-needed” basis.	
VaMS/TR/3.07	Should be able to access through Dial-Up or Broadband Connectivity.	
VaMS/TR/3.08	Should be able to support English, Odiya, Hindi and many other Indian language fonts.	
4. Network Control Software (At the USER)		
VaMS/TR/4.01	Should be able to integrate Windows / Linux based authentication services.	
VaMS/TR/4.02	Screen Layout Designer Module with Drag and Drop interface and able to support more than 2 Media Zones, 3 Scrolling Zones, Date and time zone along with Weather Module for any screen resolution in both the screen Formats (Portrait and Landscape).	
VaMS/TR/4.03	Alert Manager: should be able send player logs between set intervals for assigned player or Group of players through an email.	
VaMS/TR/4.04	Players (VaMS Displays) can be placed in multiple Groups and schedules can be sent to a Group or a selection of Players in a Group or to the Whole Network.	
VaMS/TR/4.05	Can add any number of media players (VaMS Displays) in the Network.	
VaMS/TR/4.06	Media zone should be able to play Videos, Flash, Images, Web pages, Office Files & PDF documents.	
VaMS/TR/4.07	Media can be organized in expandable View Folders.	
VaMS/TR/4.08	Should be able to schedule all the zones in the Screen Layout independently.	
VaMS/TR/4.09	Should have the facility to set the different shutdown time and reboot time for all days of a week for the Remote Players.	
VaMS/TR/4.10	Should have the dashboard view of the Network Connectivity Status between the Media Players (VaMS Displays) and the Central Server with current IP Address & Free Space available on Players (VaMS Displays).	
VaMS/TR/4.11	Should be able to create / delete playlist. Should be able to update playlist by adding / removing the files and also be able to modify the sequence of the files with in the playlist.	
VaMS/TR/4.12	Should be able to schedule the playlist.	
VaMS/TR/4.13	Should have the capability to log the media player start and end event with timestamp and screen shots.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
VaMS/TR/4.14	Able to generate various MIS reports such as Media Exposure between Date ranges. Should be able to export these reports in various format such as CSV, Microsoft Excel, PDF etc.	
VaMS/TR/4.15	User access & management: - Should have multi Level user access. - Able to create users and assign role based rights such as grouping the players, create Playlist, Layout Management, Reports etc.,	
VaMS/TR/4.16	Should have the log viewer module with export facility. Should have feature to provide Detailed reports related to Video/message played • Over a day with video/message play time details. • Over a week with video/message play time details. Over a month or custom selected range of days with video/message play time details.	
VaMS/TR/4.17	- Able to send Emergency messages to the players. - Emergency Messages should override the current content on the Screen and Display FULL Screen. - should have option to set the Start and End time for Emergency Messages and the frequency interval so that the player will alternate between the Emergency Messages and current content.	
VaMS/TR/4.18	Should have the option to play selected Media files using Day Time Parting (Day Parting) by providing the Start and end time for the selected Media files.	
5. Power		
VaMS/TR/5.01	Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated	
VaMS/TR/5.02	The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose	
VaMS/TR/5.03	Power Back-up & its enclosure: UPS for one hour power back-up with auto switching facility. The enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable	
VaMS/TR/5.04	Material for VaMS frame: at least 2mm aluminum or Non-corrosive, water resistant or better. Frame of the VaMS should be black & Powder coated	
6. Mounting, Installation and finishes		
VaMS/TR/6.01	Mounting structure shall use minimum 6Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VaMS sign from the Road surface	
VaMS/TR/6.02	The mounting shall be capable of withstanding road side vibrations at site of installation	
VaMS/TR/6.03	It shall be provided with suitable walkway for maintenance access	
VaMS/TR/6.04	The side interior and rear of enclosures shall be provided in maintenance free natural aluminum finish. All enclosure shall be flat and wipe clean	
VaMS/TR/6.05	Rugged locking mechanism should be provided for the onsite enclosures and cabinets	
VaMS/TR/6.06	For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency	
VaMS/TR/6.07	Wind Load: WL9 as per EN12966 to withstand high wind speeds and its own load	
7. Cabling, connections and Labelling		
VaMS/TR/7.01	All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 Cms or cable trays	
VaMS/TR/7.02	All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down	
VaMS/TR/7.03	All terminal block shall be made from self- extinguishing materials. Terminations shall be logically grouped by function and terminals carrying power shall be segregated from control signal terminals	
VaMS/TR/7.04	All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using “As built: drawings”	
VaMS/TR/7.05	Lightening arrester shall be installed for safety on each VaMS	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
VaMS/TR/7.06	The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency	
8. General		
VaMS/TR/8.01	Local Storage in VaMS: Embedded VaMS controller should be capable to store at-least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/timings, in case of connectivity failure	

Public Address System (PAS)

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. Public Address (PA) System		
PAS/TR/1.1	The PA system shall be IP based and shall provide a VoIP interface (preferred SIP based).	
PAS/TR/1.2	The system shall demonstrate through testing a speech transmission index (STI) of 0.5 or better under all operational ambient noise conditions. STI shall be demonstrated at heights of 1.5 meters above the road level at all locations using the PA-STI testing criterion.	
PAS/TR/1.3	PA announcements at each location shall be a uniformly distributed sound level on a plane 1.5 m above finished road level in all public areas that has sound pressure level (SPL) which is greater of: - 78 dB - 10 dB above ambient sound level to a maximum of 96 dB	
PAS/TR/1.4	The system shall have the capability of playing live and pre-recorded (i.e. MP3, WAV etc.) messages.	
PAS/TR/1.5	The system shall be capable of monitoring audio paths and automatic testing supervision to ensure that the systems are working as per the requirements.	
PAS/TR/1.6	All components of the PA system shall have (a) operating temperature range as per City requirement and (b) Operating and storage relative humidity as per City requirement	
PAS/TR/1.7	The system shall have a MTBF of at least 100,000 hours.	
PAS/TR/1.8	PA system shall be powered by 230 VAC, 50Hz. and the power supply units shall be of industrial grade for field devices.	
PAS/TR/1.9	The system shall provide audio processing capabilities including paging management, audio routing, equalization, digital signal processing, ambient analysis control and digital gain management.	
2. PA Speakers		
PAS/TR/2.1	The PA system speakers shall be of high impedance matching the line level input.	
PAS/TR/2.2	Speakers may have in-built amplifiers or have external amplifiers to ensure that required sound pressure levels can be achieved. Also, they shall be outdoor rated and protected against corrosion.	
3. Ambient Noise Sensors		
PAS/TR/3.1	The PA system shall provide dynamic level control and shall be fitted with ambient noise level monitoring capability to compensate for changes in noise level automatically.	
PAS/TR/3.2	The ambient noise sensor shall ensure that the output of the speakers can be automatically adjusted based on ambient noise conditions.	
PAS/TR/3.3	The Ambient noise sensors shall be connected to the Amplifier/VoIP interface to manage and optimize PA system at individual locations.	
PAS/TR/3.4	Noise sensors shall be outdoor rated and protected against corrosion	
4. Amplifier/VoIP Interface with built-in DSP		
PAS/TR/4.1	The PA system shall include amplifiers/VoIP interface capable of driving the speakers to a sound pressure level to ensure the minimum target STI of 0.5 is achieved under all conditions.	
PAS/TR/4.2	The Amplifier/VoIP interface shall be installed at the intersections or locations as per the detailed design requirements.	
PAS/TR/4.3	The VoIP should have an output power of minimum 60W (RMS).	
PAS/TR/4.4	The VoIP interface should have an input for noise sensor to monitor ambient noise.	

PAS/TR/4.5	The device shall convert analog audio to standard IP format for transmission over the Ethernet based fibre optic network.	
PAS/TR/4.6	The device shall support browser based configuration to allow control and monitoring from any network-based PC.	
PAS/TR/4.7	The device shall provide at least 4 inputs and 6 relay outputs to interface with external systems.	
PAS/TR/4.8	The device should have LED status indications for faults including but not limited to power, short circuit etc.	
5. PAS Operator Consoles		
PAS/TR/5.1	The operator console shall be located in the ICCC and shall be IP based system.	
PAS/TR/5.2	The console shall have hot keys for all call, individual call and group functions call for selecting multiple locations.	
PAS/TR/5.3	The operator console shall have control desk functions.	
6. UPS for PA System		
PAS/TR/6.1	The UPS unit shall be on-line 3:3 or 3:1 phase UPS with extendable rack system.	
PAS/TR/6.2	The UPS design shall ensure that a single component/ device failure shall not result in failure of the entire UPS system. The design of UPS System shall be modular to permit easy maintenance.	
PAS/TR/6.3	The UPS system shall have maximum humming noise level of 65 DB one meter away from the UPS cabinets. This shall not exceed 69 dBA measured 5 feet from surface of the UPS.	

Environmental Monitoring System (EMS)

Context

Regional Pollution Control Board, Rourkela monitors the pollution level through two environment monitoring stations located at (i) Regional Office Building, Sector-5 and (ii) IDL colony, Sonaparbat in Rourkela. Key parameters monitored at these stations include Sulphur Dioxide (SO_2), Oxides of Nitrogen (NO_2), Suspended Particulate Matter (SPM) and Respirable Suspended Particulate Matter (RSPM/PM10) apart from temperature and humidity. The sensors used for monitoring in these facilities are fixed and immovable. Currently, the readings are recorded manually and shared with State Pollution Control Board (SPCB) and Central Pollution Control Board (CPCB).

An analysis of the existing environment monitoring system presents the following key issues:

- Manual reading and noting of the parameters which may result in inaccuracy.
- All the critical parameters viz. Ozone, Carbon Monoxide, Wind Speed, Rainfall, Noise, etc. are not getting captured.
- No alert system for deviation of parameters from standard values.
- Absence of Public Information System at public places to provide real-time information to the citizens on environment parameters.
- Absence of data analytics for decision making based on values of parameters recorded.

Objectives

In order to provide real time information on environmental parameters to the citizens and to enable the concerned authority to establish priorities for reduction and control of pollutant level by undertaking preventive and corrective measures, it is proposed to set up Environment Monitoring Systems (EMS) at strategic locations across the city.

Key benefits envisaged from installation of EMS will include:

- Real-time view of environment parameters in VaMS installed at different strategic locations.
- Necessary corrective measures can be taken in the event of any major deviation in the values of parameters to improve the pollution levels.

Scope of Work

MSI shall require to design and install the environmental sensors at 5 strategic locations to display environment related information through Variable Message Display Boards. The environment sensors shall be integrated with the central control system at ICCC to capture and display/ provide feed on Temperature, Humidity, and Pollutants etc. The data collected shall be location-marked. Each environmental Sensor should be able to measure following parameters:

- Carbon Monoxide (CO) sensor
- Ozone (O3) sensor
- Nitrogen Dioxide (NO2) sensor
- Sulphur Dioxide (SO2) sensor
- Carbon Dioxide (CO2) sensor
- Particulate/SPM Profile (PM10 and PM2.5) sensor
- Temperature sensor
- Relative Humidity sensor
- Wind Speed sensor
- Wind Direction sensor
- Rainfall sensor
- Barometric Pressure sensor
- Noise sensor

Key elements of the proposed EMS solution are as follows:

- **Environmental Sensors** which will monitor the air quality parameters with sensors being calibrated remotely and visible as a layer in the GIS map
- **System software** shall take input data from environmental Sensors, process the same using data analytics at ICCC and feed the data into Digital Display Screen (DDS). It shall also monitor the trends and identify

deviations, if any.

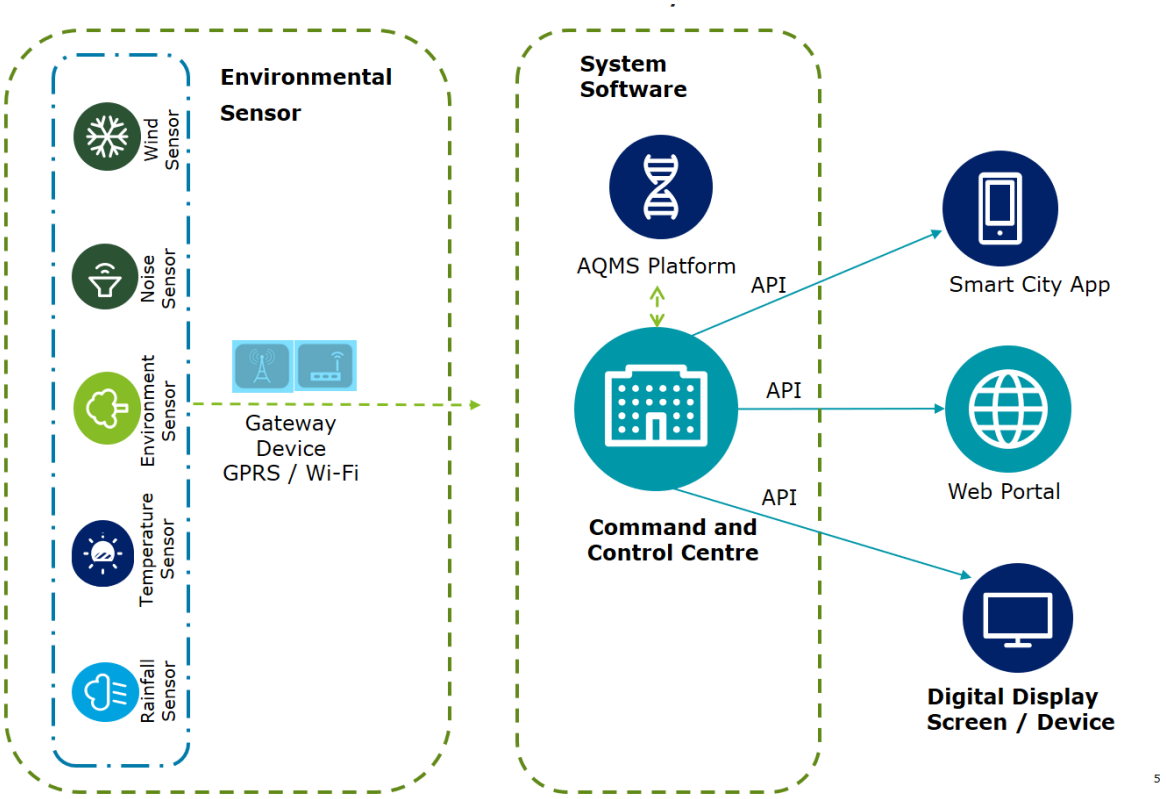
- **Digital Display Screen** (DDS) shall display the environment parameters by taking inputs from the application at the ICCC

A total of 5 (Five) locations have been identified for installation of Environment Monitoring Systems which is highlighted in the table below:

No.	Proposed Locations
1	Bisra Chowk
2	Chhend Chowk
3	Vedvyas Chowk
4	Sector -19 IGH Chowk
5	Industrial Area near Jail

Indicative Solution Architecture

An indicative solution architecture proposed for the installation of Environmental Monitoring System (EMS) to enhance monitoring of the air quality parameters in the city is presented in the figure below:



The environmental sensors at various strategic locations shall capture the relevant parameters and transmit the data to the ICCC. Data analytics shall be applied on the data using the EMS system installed at the ICCC. The required air quality parameters including temperature, Carbon Monoxide, rainfall, noise, etc. shall then be broadcast through various delivery channels like Smart City App, Web Portal and Digital Display Screens installed at various places of the city to provide requisite information to the citizens.

Minimum Functional Requirements

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
1. Environmental Sensors & Sensor Station		
EMS/FR/1.1	The environmental sensors housed in the Sensor station shall monitor following	

S. No.	Minimum Functional Requirements	Compliant (Yes / No)
	parameters and include the following integrated sensors inside one station: - Carbon Monoxide (CO) sensor - Ozone (O3) sensor - Nitrogen Dioxide (NO2) sensor - Sulphur Dioxide (SO2) sensor - Carbon Dioxide (CO2) sensor - Particulate/SPM Profile (PM10 and PM2.5) sensor - Temperature sensor - Relative Humidity sensor - Wind Speed sensor - Wind Direction sensor - Rainfall sensor - Barometric Pressure sensor - Noise sensor	
EMS/FR/1.2	The sensors shall be able to communicate its data using wireless technology. Environmental sensors can also be connected via 3G or 4G wireless network or Wi-Fi networks. It is not mandatory to connect all sensors via fibre network.	
EMS/FR/1.3	Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform.	
EMS/FR/1.4	The environmental sensors location shall be visible as a layer in GIS Maps.	
EMS/FR/1.5	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air and noise quality among other parameters as detailed above.	
EMS/FR/1.6	Environmental sensor station shall be ruggedized enough to be deployed in open air areas such as streets and parks.	
EMS/FR/1.7	Mounting of the environmental sensor module shall be co-located on street light pole or shall be installed on a tripod stand or a standalone pole.	
2. System software		
EMS/FR/2.1	Environmental sensor station shall have a pre-installed software.	
EMS/FR/2.2	Software shall display real time and historical data in chart and table views for dashboard view of the Client.	
EMS/FR/2.3	Software shall display trends of environmental parameters based on user specific time periods.	
EMS/FR/2.4	It shall be possible to configure and calibrate the sensors through the software from a remote location.	
EMS/FR/2.5	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.	
3. Digital Display Screen (DDS)		
EMS/FR/3.1	DDS will be installed at identified strategic location and will be used for display environmental parameters along with other promotional messages. The integrated DDS software application will allow user to publish specific messages & general informative messages.	
EMS/FR/3.2	DDS shall be integrated with the environmental station for automatically displaying information from environmental sensors.	
EMS/FR/3.3	A DDS software system shall be provided to the CCC for message preparation monitoring and control of the DDS. The DDS will communicate with ICCC using an IP based network.	
EMS/FR/3.4	DDS software application will provide the normal operator to publish predefined sets of messages (textual / image) along with information from environmental sensors. The application shall have an option for supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.	
EMS/FR/3.5	DDS software application will accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client. Software should be GUI based, and capable to handle upto 10 DDS signage. User should be able to select desired location in Map and this should enable user to see the live status of that specific DDS.	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. Environmental Sensors & Sensor Station		
General		
EMS/TR/1.1	Each environmental sensor shall be housed in modules and further integrated into one single enclosure.	
EMS/TR/1.2	The design shall be modular in nature which shall have the capability to add additional environmental sensors in the future into the enclosure.	
EMS/TR/1.3	Data of all the environmental sensor shall be available on the same software interface.	
EMS/TR/1.4	It shall be possible to remove or replace individual sensor modules without affecting the functioning of rest of the system.	
EMS/TR/1.5	It shall be possible to mount the air quality monitoring station to a pole, tripod or wall mounting brackets.	
Carbon Monoxide (CO) Sensor		
EMS/TR/1.6	Range of CO sensor shall be between 0 to 1000 PPM.	
EMS/TR/1.7	Resolution of CO sensor shall be 0.01 PPM or better.	
EMS/TR/1.8	Lower detectable limit of CO sensor shall be 0.040 PPM or better.	
EMS/TR/1.9	Precision of CO sensor shall be less than 3% of reading or better.	
EMS/TR/1.10	Linearity of CO sensor shall be less than 1% of full scale or better.	
EMS/TR/1.11	Response time of CO sensor shall be less than 60 seconds.	
EMS/TR/1.12	Operating temperature of CO sensor shall be as per City requirement	
EMS/TR/1.13	Operating pressure of CO sensor shall be ±10%.	
Ozone (O3) Sensor		
EMS/TR/1.14	O3 Sensor shall have a range of at least 0-1000 PPB.	
EMS/TR/1.15	Resolution of O3 sensor shall be 10 PPB or better.	
EMS/TR/1.16	Lower detectable limit of O3 sensor shall be 10 PPB or better.	
EMS/TR/1.17	Precision of O3 sensor shall be less than 3% of reading or better.	
EMS/TR/1.18	Linearity of O3 sensor shall be less than 1% of full scale.	
EMS/TR/1.19	Response time of O3 sensor shall be less than 60 seconds.	
EMS/TR/1.20	Operating temperature of O3 sensor shall be as per City requirement	
EMS/TR/1.21	Operating pressure of O3 sensor shall be ±10%.	
Nitrogen Dioxide (NO2) Sensor		
EMS/TR/1.22	NO2 Sensor shall have a range of at least 0-10 PPM.	
EMS/TR/1.23	Resolution of NO2 sensor shall be 0.001 PPM or better.	
EMS/TR/1.24	Lower detectable limit of NO2 sensor shall be 0.001 PPM or better.	
EMS/TR/1.25	Precision of NO2 sensor shall be less than 3% of reading or better.	
EMS/TR/1.26	Linearity of NO2 sensor shall be less than 1% of full scale.	
EMS/TR/1.27	Response time of NO2 sensor shall be less than 60 seconds.	
EMS/TR/1.28	Operating temperature of NO2 sensor shall be as per City requirement	
EMS/TR/1.29	Operating pressure of NO2 sensor shall be ±10%.	
Sulphur Dioxide (SO2) Sensor		
EMS/TR/1.30	SO2 Sensor shall have a range of at least 0-20 PPM.	
EMS/TR/1.31	Resolution of SO2 sensor shall be 0.001 PPM or better.	
EMS/TR/1.32	Lower detectable limit of SO2 sensor shall be 0.009 PPM or better.	
EMS/TR/1.33	Precision of SO2 sensor shall be less than 3% of reading or better.	
EMS/TR/1.34	Linearity of SO2 sensor shall be less than 1% of full scale.	
EMS/TR/1.35	Response time of SO2 sensor shall be less than 60 seconds.	
EMS/TR/1.36	Operating temperature of SO2 sensor shall be as per City requirement	
EMS/TR/1.37	Operating pressure of SO2 sensor shall be ±10%.	
Carbon Dioxide (CO2) Sensor		
EMS/TR/1.38	CO2 Sensor shall have a range of at least 0-5000 PPM.	
EMS/TR/1.39	Resolution of CO2 sensor shall be 1 PPM or better.	
EMS/TR/1.40	Lower detectable limit of CO2 sensor shall be 10 PPM or better.	
EMS/TR/1.41	Precision of CO2 sensor shall be less than 3% of reading or better.	
EMS/TR/1.42	Linearity of CO2 sensor shall be less than 2% of full scale.	
EMS/TR/1.43	Response time of CO2 sensor shall be less than 60 seconds.	
EMS/TR/1.44	Operating temperature of CO2sensor shall be as per City requirement	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
EMS/TR/1.45	Operating pressure of CO2 sensor shall be ±10%.	
Particulate Profile Sensor		
EMS/TR/1.46	Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air.	
EMS/TR/1.47	Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better.	
EMS/TR/1.48	Range of PM10 shall be 0 to 450 micro gms / cu.m or better.	
EMS/TR/1.49	Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3.	
EMS/TR/1.50	Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading).	
EMS/TR/1.51	Flow rate shall be 1.0 LPM or better.	
EMS/TR/1.52	Operating temperature of the sensor shall be as per City requirement	
EMS/TR/1.53	Operating pressure of the sensor shall be ±10%.	
Temperature Sensor		
EMS/TR/1.54	Temperature sensor shall have the capability to display temperature in °Celsius.	
EMS/TR/1.55	Temperature range shall be -10° to +100°C.	
EMS/TR/1.56	Sensor accuracy shall be ±0.3°C (±0.5°F) or better.	
EMS/TR/1.57	Update interval shall be 10 to 12 seconds.	
Relative Humidity Sensor		
EMS/TR/1.58	Range of relative humidity sensor shall be 1 to 100% RH.	
EMS/TR/1.59	Resolution and units of relative humidity sensor shall be 1% or better.	
EMS/TR/1.60	Accuracy of the sensor shall be ±2% or better.	
EMS/TR/1.61	Update interval shall be less than 60 seconds.	
EMS/TR/1.62	Drift shall be less than 0.25% per year.	
Wind Speed Sensor		
EMS/TR/1.63	Wind speed sensor shall have the capability of displaying wind speed in km/h or knots.	
EMS/TR/1.64	Range of sensor shall be 0-60 m/s.	
EMS/TR/1.65	Accuracy of wind speed sensor shall be ±5% or better.	
EMS/TR/1.66	Update interval shall be less than 60 seconds.	
Wind Direction Sensor		
EMS/TR/1.67	Range of the wind direction sensor shall be 0° to 360°.	
EMS/TR/1.68	Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display.	
EMS/TR/1.69	Accuracy shall be ±3% or better.	
EMS/TR/1.70	Update interval shall be 2.5 to 3 seconds.	
Rainfall Sensor		
EMS/TR/1.71	Rainfall sensor shall the capability of displaying level of rainfall in inches and millimetre.	
EMS/TR/1.72	Daily Rainfall range shall be 0 to 99.99” (0 to 999.8 mm).	
EMS/TR/1.73	Monthly/yearly/total rainfall range shall be 0 to 199” (0 to 6553 mm).	
EMS/TR/1.74	Accuracy for rain rates shall be up to 4”/hr (100 mm/hr) or ±4% of total.	
EMS/TR/1.75	Update interval shall be less than 60 seconds.	
EMS/TR/1.76	0.02” or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event.	
Barometric Pressure Sensor		
EMS/TR/1.77	Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa/mb.	
EMS/TR/1.78	Range of barometric pressure sensor shall be 540 hPa/mb to 1100 hPa/mb.	
EMS/TR/1.79	Elevation range of the barometric pressure sensor shall be -600 m to 4570 m.	
EMS/TR/1.80	Uncorrected reading accuracy shall be ±1.0 hPa/mb at room temperature or better.	
EMS/TR/1.81	Elevation accuracy shall be ±10’ (3m) to meet equation accuracy specification or better.	
EMS/TR/1.82	Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa/mb) or better.	
EMS/TR/1.83	Update interval shall be less than 60 seconds.	
Noise Sensor		
EMS/TR/1.84	Noise sensor shall detect the intensity of the ambient sound in a particular area.	
EMS/TR/1.85	Noise Sensors shall be installed for the outdoor applications.	
EMS/TR/1.86	Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA.	
EMS/TR/1.87	Noise sensor shall have resolution of 0.1 dBA.	
Environmental Requirements		
EMS/TR/1.88	Enclosure shall be rugged weather proof IP65 rated and shall house the power modules,	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	thermal management system, embedded PC and user configured analyser modules as well.	
EMS/TR/1.89	Environmental operating range shall be 0°C to +60°.	
Electrical Requirements		
EMS/TR/1.90	Power requirements of the system (environmental station and DDS) shall 220-240 VAC, 50Hz. It shall have an in-built NEMA 5-15P plug factory installed.	
EMS/TR/1.91	All modules inside the enclosure shall operate from 12VDC power. The MSI shall be responsible for any power conversions required for operations of this system.	
Networking Requirements		
EMS/TR/1.92	Environmental station and DDS shall support communications by GPRS (2G) / GSM (3G) / LTE (4G) / Wi-Fi / LORA Sensors shall have provision to interchange between GSM and LORA.	
2. System Software		
EMS/TR/2.1	Software shall be pre-installed on every built system.	
EMS/TR/2.2	It shall be possible to connect to the station using internet browser on computer tablet or mobile without any need of installing software for viewing information.	
EMS/TR/2.3	Software shall display real-time and historical data in chart and table views.	
EMS/TR/2.4	Software shall display trends of environmental parameters based on user specified time periods.	
EMS/TR/2.5	It shall be possible to configure and calibrate the sensors through the software from a remote location.	
EMS/TR/2.6	Software shall display and export sensor diagnostic information.	
EMS/TR/2.7	User shall be able to change sensor module settings through the software and from remote locations.	
EMS/TR/2.8	Administrator shall be able to manage access privileges for only authorized users.	
EMS/TR/2.9	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.	
EMS/TR/2.10	It shall be integrated at the ICCC for the purposes of monitoring, display of information and control of the system.	
EMS/TR/2.11	Software shall be integrated with e-Governance applications such as City portal and City applications. Real time environmental information shall be published on these portal as part of open data initiative.	
3. Digital Display Screen (DDS)		
EMS/TR/3.1	The DDS shall be installed at location identified by Client. The DDS shall be outdoor rated.	
EMS/TR/3.2	DDS shall have be True Colour. Text on the DDS shall be readable in bright sunlight.	
EMS/TR/3.3	The pixel pitch of DDS shall be minimum 5mm.	
EMS/TR/3.4	The model size of DDS shall be minimum 160X160 mm.	
EMS/TR/3.5	The model pixel of DDS shall be minimum 32X32 Pixels.	
EMS/TR/3.6	The lattice density of DDS shall be minimum 40000 dots/square meter.	
EMS/TR/3.7	The viewing distance shall be between 4m to 30m. The screen size shall be proposed accordingly to ensure that the character height is at least 50mm.	
EMS/TR/3.8	The average power consumption shall not exceed the 500W/square meter.	
EMS/TR/3.9	The refresh frequency of DDS shall be ≥ 400HZ.	
EMS/TR/3.10	The horizontal view angle shall be > 110 degree.	
EMS/TR/3.11	The working temperature shall be as per City requirement	
EMS/TR/3.12	The working voltage shall be not more than DC 5V.	
EMS/TR/3.13	The MTBF of DDS shall not be less than 100,000 hours.	
EMS/TR/3.14	The gray scale shall be 12 bit/ 1 colour.	
EMS/TR/3.15	The Brightness shall be 6500 cd/square meter.	
EMS/TR/3.16	The blind spot rate shall be minimum < 0.00001.	
EMS/TR/3.17	The IP rating shall be minimum IP66 for front as well as rear.	
EMS/TR/3.18	Message shall be readable even in broad daylight without any shade & displayed image shall not appear to flicker to the normal human eye (>6000 cd/m2).	
EMS/TR/3.19	The Display capability of DDS shall be fully programmable, full colour, full matrix, LED displays & shall have Alpha-numeric, Pictorials, Graphical & video capabilities.	
EMS/TR/3.20	The Display Language shall be support both pictograms and bilingual (English and	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	Devanagari) text.	
EMS/TR/3.21	The Display Front Panel shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean & shall be 100% anti-glare.	
EMS/TR/3.22	The message Creation shall be through both CCC Application and locally.	
EMS/TR/3.23	The DDS shall support Multilingual (Odiya/English/Hindi etc.) languages and all fonts supported by Windows.	
EMS/TR/3.24	The DDS shall have the facility of auto dimming adjusts to ambient light level.	
EMS/TR/3.25	The Display size of DDS shall be minimum 70 inches diagonal.	
EMS/TR/3.26	The DDS shall have the access control mechanism so that the usage is regulated.	
EMS/TR/3.27	The DDS shall be wall, Pole & gantry mounted. The mounting accessories shall be the part of DDS.	
EMS/TR/3.28	The DDS shall have automatic on/off operation.	

Wi-Fi Hotspots

Key Objectives

In order to reduce digital divide and provide urban dwellers with a high speed and seamless network connectivity, Wi-Fi hotspots are proposed to be installed at select public places across the city of Rourkela to enable citizens to collaborate and perform business activities on the go. Key benefits envisaged from city Wi-Fi hot spot includes the following:

- Bridge the gap between the digital divide by providing access to internet to people who cannot afford the same.
- Improve the image of the city by access to information and services through the city Wi-Fi network
- Provide city administration efficient access to mobile applications that support their individual work processes, from building inspections to solid waste removal, and municipal services.

Scope of Work

Key elements of the proposed Wi-Fi hotspots are as follows:

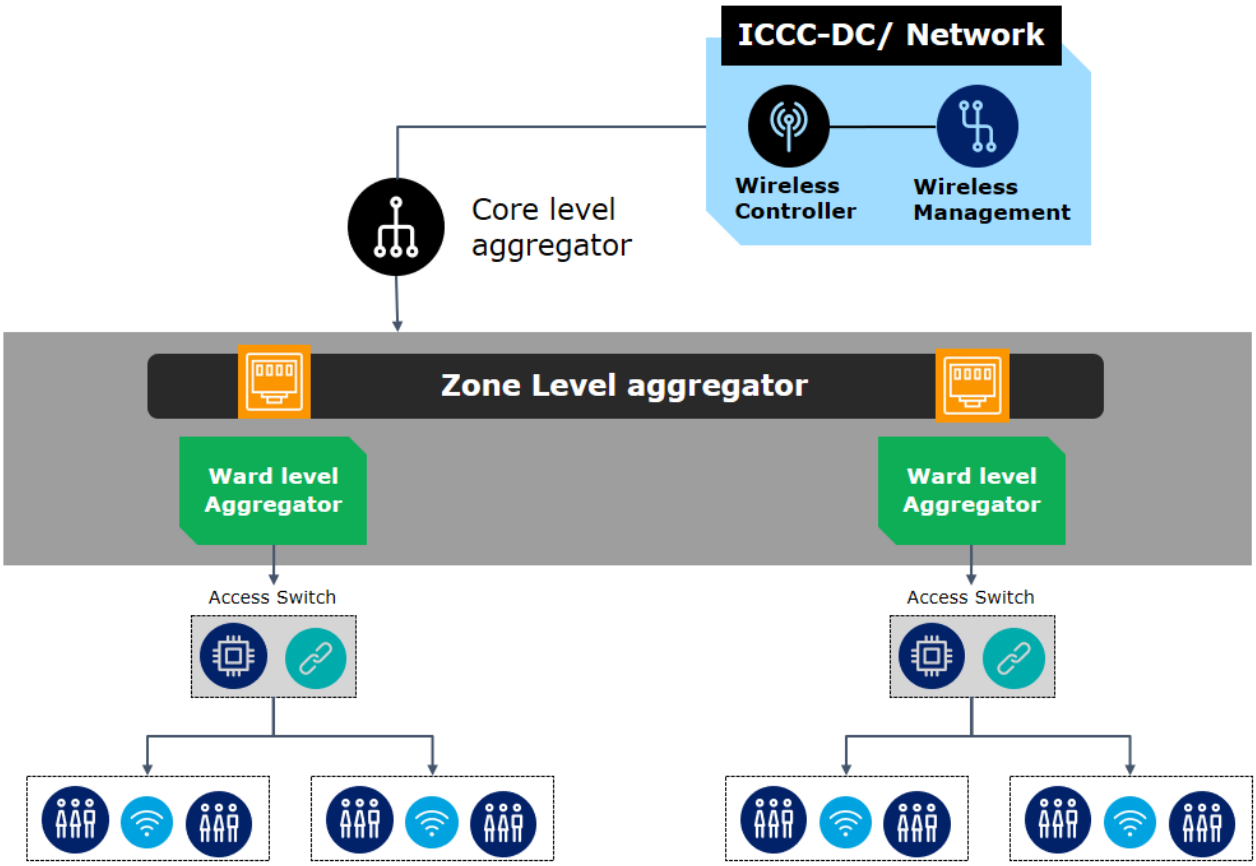
- Multiple Access Points at each selected location for citizens to access Wi-Fi.
- Wi-Fi network shall include Wi-Fi controller to monitor, manage, and control access points from the ICCC.
- Centralised Wi-Fi management software and application system to monitor, analyse, and configure wireless network in automatic fashion.
- Highly secure user login authentication using mobile number and plans for excess usage beyond free data limits.
- The Wi-Fi network shall have built-in encryption mechanism to encrypt all communications and data transfer over the Wi-Fi for all the users of Wi-Fi.
- Online UPS to ensure that a single component/ device failure shall not result in failure of the entire UPS system.

A total of 13 locations have been identified for installation of Wi-Fi Hotspots as highlighted in the table below:

S. No	Proposed Wi-Fi Hotspot Locations
1.	Central Park, Near BSNL chowk, Chhend Colony, Rourkela
2.	E-Library, Uditnagar, Rourkela
3.	Rourkela Municipal Corporation, Uditnagar
4.	Rourkela Development Authority, Uditnagar
5.	Proposed Panposh Market, Panposh Chowk
6.	Rourkela Government Hospital, Panposh Road,
7.	Proposed Brahmani Riverfront Development, Panposh
8.	Indra Gandhi Park, Sector 4, Rourkela
9.	Biju Pattnaik Sports Complex, Panposh,
10.	Birsa Stadium, Birsa Chowk, Rourkela
11.	New Bus stand, Rourkela
12.	Children's Park, Uditnagar, Rourkela
13.	Deer Park, Sector-8 , Rourkela

Indicative Solution Architecture

A high level schematic diagram proposed for the Wi-Fi hotspots to enhance access to high speed and network connectivity to the citizens in the city is depicted below:



As reflected in the figure above, the city wide Wi-Fi solution shall be managed by the Wireless Management System (WMS) hosted at the Data Center of the ICCC. On receiving the instructions from WMS, the wireless controller shall configure the field level aggregators and switches. The citizens will get connected to the Access Points (APs) for accessing the internet connectivity.

Minimum Functional Requirements

S.No	Minimum Functional Requirements	Compliant (Yes / No)
Wifi/FR/1.01	The objective is to provide strong, seamless and highly available Wi-Fi for citizens to collaborate and perform business activities on the go. Wi-Fi services will also reduce the digital divide and provide urban dwellers within Rourkela a better & faster means for connectivity	
Wifi/FR/1.02	City Wi-Fi internet access shall be free in select areas in the city, with a maximum download limit and/ or time of usage to be defined as per client requirement, after which City Wi-Fi services will be available on a paid basis. Offered solution shall allow wireless access through various kinds of devices such as smart phones, laptops, tablets, and desktops. All e- governance applications by RMC, state government and central government shall be excluded from this download limit.	
Wifi/FR/1.03	City Wi-Fi will be made available to citizens at minimum five (5) Mbps speed with a minimum throughput of 512kbps. Free City Wi-Fi facility should be available as per the specified in SLAs in the RFP for a specified time.	
Wifi/FR/1.04	MSI should ensure that the citizen should be able to use same access details (login id/ username and password) even if he/she moves from one wifi spot zone to another to provide unified experience of connectivity for the citizen	

S.No	Minimum Functional Requirements	Compliant (Yes / No)
Wifi/FR/1.05	The MSI shall impose restrictions on access and download from malicious sites for City Wi-Fi users. Such sites shall be as notified by TRAI/ regulatory agencies and also be notified to MSI from time to time by the client	
Wifi/FR/1.06	A denied URL list should be applied on this City Wi-Fi SSID and should be updated on a run time basis, to self-learn (no human inference shall be required) and automatically update the list. Any malicious user on the City Wi-Fi should be immediately dropped and blocked after appropriate recording of the evidence	
Wifi/FR/1.07	After the free usage of as defined by client, user shall automatically switch over to login page and continue to use by paying as per the data plans else the user will not have the internet access. The rates for Paid City Wi-Fi and wired internet services should be competitive to the market rates of the leading data service providers in Odisha. MSI should obtain client approval before introducing these rates and any proposed changes in the rates.	
Wifi/FR/1.08	MSI will be responsible for design and engineering of all the network components to meet coverage and capacity requirements of hotspots based on following parameters: Area of Wi-Fi hotspot, Peak load and Density of user devices/ concurrent users/Connections required in the area. MSI should test the entire location and ensure availability of the Wi- fi services before declaring it ready for rollout to the client	
Wifi/FR/1.09	Based on the hotspots capacity requirements, MSI shall determine and provide number of Access points per Hotspot as per the required Internet bandwidth (both per Hotspot and per user) and aggregated total bandwidth per hotspot. Applicant can consider the contention ratio of 1:10 per user from day 1 of implementation of the project	
Wifi/FR/1.10	MSI should assure compliance with All DoT/ TRAI / statutory guidelines/ court orders including all amendments issued from time to time, for the services rendered by them including and not limited to security, including registration of users for accessing the public Wi-Fi	
Wifi/FR/1.11	Client (RSCL/ RMC) shall not be responsible for any violation of guidelines at any given point of time. The MSI is liable for all compliances as required	
Wifi/FR/1.12	MSI should ensure appropriate bandwidth allocation for free and paid Wi-Fi users as well for carrying data for all the sub systems with built in scalability for enhanced usage needs in the future. If Wi-Fi technology is changed during the contract period to any other technology, the same has to be provided by the MSI.	
Wifi/FR/1.13	MSI should ensure the security of the Wi-Fi network and should be able to monitor and manage using appropriate access login controls and audit trails from the Smart City Operations Center. It should be approved by the client before actual implementation of the same	
Wifi/FR/1.14	All the Applicants are required to conduct a site survey to address coverage and capacity requirements throughout the areas where hotspots are to be created at their own cost. The coverage maps, where hotspot is to be created, shall be prepared by the Successful Bidder it should be approved by the client before actual implementation of the same	
Wifi/FR/1.15	MSI should ensure to put up a system in place which can control each registered user's access to Wi-Fi network and the MAC address of the device. Necessary security measures should be enforced along with access control policies and tracking & auditing the usage	
Wifi/FR/1.16	Solution shall be able to restrict the bandwidth as per the policies. Solution shall have configurable GUI for Policy management to differentiate location wise Bandwidth policies	
Wifi/FR/1.17	The solution shall support Usage based on data usage as well as time duration based monitoring. It shall support real time disconnection based on usage of time or data	
Wifi/FR/1.18	The application should be IPv4 and IPv6 compliant.	

S.No	Minimum Functional Requirements	Compliant (Yes / No)
Wifi/FR/1.19	It shall offer complete subscriber management features in Subscriber Management options which mainly focuses on creating, editing, updating, renewing, deleting, and managing of accounts for all subscribers.	
Wifi/FR/1.20	The database for the system is to be provided by the vendor along with the required hardware, software, etc. to maintain logs as per TRAI guidelines issued time to time.	
Wifi/FR/1.21	All Government advertisement and Government schemes should be published free of cost on the login pages/landing pages. Client shall take the control of operations in case of any disaster/emergency situations and the MSI shall operate under the directions of the appointed authority	
Wifi/FR/1.22	As part of this implementation exercise, the client should get the intelligence about the Wi-Fi service through statistical data, reports and analysis of User registration, Data Usage under various schemes, Network status across the city, device availability, throughput of the internet, Hardware status across the city etc.	
Wifi/FR/1.23	MSI should provide a web portal for the client to monitor the mentioned indicators and to conduct the necessary audit of implemented system.	
Wifi/FR/1.24	Client web portal should have a functionality to retrieve various MIS reports. E.g.: a. User wise, Access point wise, connectivity and data usage report in digital format from systems, security events, forensic auditing in given format. b. Other relevant reports as may be required by client, should have to be provided by the Successful Bidder. c. Blacklisting of users by MAC Address or by checking malicious activity performed by user should be achieved	

Minimum Technical Requirements

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
1. Key features of Wi-Fi Access points (AP)		
Wifi/TR/1.01	The network and access points should support creation of robust and reliable mesh network topology based on the field surveys of areas of Rourkela (RMC Areas).	
Wifi/TR/1.02	MSI should perform a detailed survey in RMC area to determine the number of APs required and accordingly configure the number of concurrent users per access point, in a way that there is a fair balance between the hardware costs per AP versus bandwidth cost	
Wifi/TR/1.03	The proposed Wired/ wireless and Wi-Fi network architecture should adhere to industry recommended design standards and state of art technology.	
Wifi/TR/1.04	APs should be installed in outdoor areas and provide last mile connectivity. AP should comply key International and Indian standards for safety, including RF radiations. APs should protect internally stored configuration information.	
Wifi/TR/1.05	Case-covering should be there for the AP but leaving the antenna out (if external antennas are there) to achieve anti-theft protection.	
Wifi/TR/1.06	To maintain consistent quality of service for users, network traffic should be prioritized according to applications/users and handled in the AP/Controllers or upstream devices so that critical traffic is processed immediately and network congestions are avoided.	
Wifi/TR/1.07	Access Points proposed shall be 802.11ac, Wave 2 compliant, include radios for both 2.4 GHz and 5 GHz.	
Wifi/TR/1.08	AP shall support dual band antenna ports.	
Wifi/TR/1.09	Shall have -100 dB or better Receiver Sensitivity.	
Wifi/TR/1.10	Shall support 2X2 multiple-input multiple-output (MIMO) with two spatial streams.	
Wifi/TR/1.11	Shall support 802.11ac, Wave 2 and backward compatible with 802.11n standards.	
Wifi/TR/1.12	Shall support data rates upto 860 Mbps on 5Ghz radio.	
Wifi/TR/1.13	Shall support 80 MHz wide channels in 5 GHz.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
Wifi/TR/1.14	Shall support WAP enforced load-balance between 2.4Ghz and 5Ghz band.	
Wifi/TR/1.15	The Wireless Backhaul/Mesh shall operate in 5Ghz.	
Wifi/TR/1.16	Support Encrypted and authenticated connectivity between all backhaul components.	
Wifi/TR/1.17	Access point should have wired uplink interfaces including one 10/100/1000BASE-T Ethernet autosensing (RJ-45).	
Wifi/TR/1.18	Wireless AP should support beam-forming technology to improve downlink performance of all mobile devices, including one-, two-, and three-spatial stream devices on 802.11ac without taking the inputs from client.	
Wifi/TR/1.19	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.	
Wifi/TR/1.20	Shall incorporate radio resource management for power, channel, coverage whole detection and performance optimization.	
Wifi/TR/1.21	Access point shall support powering from AC /DC/ POE/PoE+.	
Wifi/TR/1.22	Access point shall support pole, wall and Cable strand mounting options.	
Wifi/TR/1.23	The Access point shall be IP65 or better.	
Wifi/TR/1.24	The Access point shall support operating temperature as per City requirement	
Wifi/TR/1.25	WiFi Alliance Certification for WMM and WMM power save.	
Wifi/TR/1.26	Shall support QoS and Video Call Admission Control capabilities.	
Wifi/TR/1.27	Shall support Spectrum analysis including @ 80 MHz.	
Wifi/TR/1.28	Same model AP that serves clients shall be able to be dedicated to monitoring the RF environment.	
Wifi/TR/1.29	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.	
Wifi/TR/1.30	Shall support 16 WLANs per AP for BSSID deployment flexibility.	
Wifi/TR/1.31	Shall support telnet and SSH login to APs directly for troubleshooting flexibility.	
2. Minimum Requirements of Wi-Fi Network System:		
Wifi/TR/2.01	MSI has to offer the Wi-Fi management services. The Wi-Fi management system should be capable of performing the following functions: Configuration, enabling-disabling of Access Points as and when required. It shall have centralized Database which enables administrator easily manage database from a single point in distributed Architecture Real-time reporting: • Give summary of wireless system status on single management console with graphical user interface which can be customized for future use Inventory of Access Points and their current status. • No of APs connected to the network / switches/ repeaters etc. with hierarchy of controls (with IP) as per the design of the Successful Bidder • No of users connected to AP with IP of access Points.	
3. Key features of Wi-Fi Controllers		
Wifi/TR/3.01	The WLAN controllers should be, capable of managing at least 1500 Wireless AP and should be scalable as and when required.	
Wifi/TR/3.02	The controller solution should facilitate monitoring, management, control, and up-gradation from the centralized Smart City Operations Center.	
Wifi/TR/3.03	The controllers should communicate back and forth with the centralized security system and network management system in real time.	
Wifi/TR/3.04	Should be compliant with IEEE CAPWAPor equivalent for controller-based WLANs	
Wifi/TR/3.05	Should have at least 4 x 10 Gigabit Ethernet interface.	
Wifi/TR/3.06	Should support both centralized as well as distributed traffic forwarding architecture with L3 roaming support from day 1. Should have IPv6 ready from day one.	
Wifi/TR/3.07	Controller should have hot-swappable redundant power supplies.	
Wifi/TR/3.08	Controller should be capable of supporting both 1G and 10 G SPFs on same Network I/O ports.	
Wifi/TR/3.09	WLAN Controller should support minimum of 6000 Access points in a single chassis. If any OEM/Bidder can't provide WLAN controller to support 6000 AP in 2RU form	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
	factor, multiple controllers should be proposed to meet the requirement from day one. Proposed controller should support 1+1/N+1 redundancy from day one.	
Wifi/TR/3.10	Should be rack-mountable. Required accessories for rack mounting to be provided.	
Wifi/TR/3.11	WLC should support AVC functionality on local switching architecture.	
Wifi/TR/3.12	WLC should support AC and DC powering options.	
Wifi/TR/3.13	WLC should support AP License Migration from one WLC to another.	
Wifi/TR/3.14	Should support minimum 4000 VLANs.	
Wifi/TR/3.15	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients.	
Wifi/TR/3.16	WLC should support guest-access functionality for IPv6 clients.	
Wifi/TR/3.17	Should support IEEE 802.1p priority tag.	
Wifi/TR/3.18	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.	
Wifi/TR/3.19	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.	
Wifi/TR/3.20	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.	
Wifi/TR/3.21	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused.	
Wifi/TR/3.22	Should support minimum 500 WLANs.	
Wifi/TR/3.23	Should support dynamic VLAN assignment.	
Wifi/TR/3.24	Should able to do dynamic channel bonding based on interference detected on particular channel.	
Wifi/TR/3.25	Should support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac.	
Wifi/TR/3.26	Should provide visibility to Network airtime in order to set the airtime policy enforcement.	
Wifi/TR/3.27	Should be able to restrict the number of logins per user.	
Wifi/TR/3.28	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.	
Wifi/TR/3.29	Should support MAC authentication to provide simple authentication based on a user's MAC address.	
Wifi/TR/3.30	WLC Should support Rogue AP detection, classification and standard WIPS signatures.	
Wifi/TR/3.31	The controller shall be able to detect employee device connection to Rogue Access Point and contain it automatically.	
Wifi/TR/3.32	WLC should be able to exclude clients based on excessive/multiple authentication failure.	
Wifi/TR/3.33	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic.	
Wifi/TR/3.34	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.	
Wifi/TR/3.35	Should support AP location-based user access to control the locations where a wireless user can access the network.	
Wifi/TR/3.36	Should support Public Key Infrastructure (PKI) to control access.	
Wifi/TR/3.37	Should be able to set a maximum per-user bandwidth limit on a per-SSID basis.	
Wifi/TR/3.38	Should support SNMPv3, SSHv2 and SSL for secure management.	
Wifi/TR/3.39	Should support encrypted mechanism to securely upload/ download software image to and from Wireless controller.	
Wifi/TR/3.40	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group.	
Wifi/TR/3.41	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation.	
Wifi/TR/3.42	Should have a suitable serial console port.	
Wifi/TR/3.43	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS.	

S. No.	Minimum Technical Requirements	Compliant (Yes / No)
Wifi/TR/3.44	Controller should have Deep Packet Inspection for Layer 4-7 traffic for user for all traffic across the network to analyses information about applications usage and prioritization.	
Wifi/TR/3.45	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network.	
Wifi/TR/3.46	Should support visibility and control based on the type of applications.	
Wifi/TR/3.47	The controller failover shall not trigger client de-authentication.	
4. Key features of Backbone Network		
Wifi/TR/4.01	The public Wi-Fi network architecture design should include latest BIS, DeitY, IEEE guidelines, and WPC standards for access points	
Wifi/TR/4.02	The network should support mesh technology and provide seamless and connectivity with the controllers and backhaul network.	
Wifi/TR/4.03	Backbone Network should perform load balancing users' traffic between multiple access points (umbrella coverage) as well as different bands in an access point so that there is a fair allocation of airtime to each user.	
Wifi/TR/4.04	Backbone Network should have built-in encryption mechanism to encrypt all communications and data transfer over the Wi-Fi for all the users of Wi-Fi, for sake of security and privacy.	

Smart Classrooms

Context

With an average literacy rate[6] of 86%, the city of Rourkela has 104 Government schools[7] and 241 Private schools[8] which are divided into seven different clusters, headed by respective Cluster Resource Coordinators (CRC). Out of 104 Government schools, 27 schools are in the Area Based Development (ABD) area (Bisra Chowk to Panposh Chowk) comprising:

- 12 Primary Schools (Class 1 to 5)
- 5 Upper Primary Schools (Class 6 to 8) and,
- 10 High Schools (Class 1 to 10)

Further, a total of around 9771 students (Boys: 4681; Girls: 5090) are enrolled across these schools of which 28%, 12% and 60% of students are studying in Primary, Upper Primary and High schools respectively. The course curriculum of these schools is as per the Odisha State Board. The primary language of teaching is Odiya, with Hindi and English used as secondary languages for communication. In terms of IT infrastructure, there are computer labs across only 12 schools. In addition to these schools, there is one Observation Home in Rourkela for the temporary reception of any juvenile in conflict with law during the pendency of any inquiry regarding them. Key issues with respect to the traditional method of teaching across these schools include:

- Limited involvement of ICT related interventions prevents the students to learn from advanced interactive methods of teaching
- Non-productive time of physically drawing standard diagrams to explain its features as against readymade digital content which adversely impacts the efficiency of the teachers

Objective

Smart Classroom project envisages ICT enabled visually attractive methods of teaching to provide interactive education to students. A total of 15 classrooms are proposed to be converted into Smart classrooms across select identified schools and observation home in the ABD area of the city. Key benefits envisaged from the Smart Classrooms include:

- Reducing the non-productive time spent by teachers in doing repetitive work of drawing or preparing diagrams, and instead provide them more time in explaining its features
- Making the students acquainted of modern learning methods and instilling confidence in them for engaging

Scope of Work

The scope of work for the MSI shall include supply and installation Smart Classroom component in Government High Schools and Observation Home of Rourkela. The MSI shall be responsible for implementation of the following Smart Classroom components:

- Hardware components comprising of desktop with UPS, projector for delivering the content and interactive whiteboard for projecting content to the students
- Networking components comprising the router which shall provide the necessary network connectivity for delivering the updated content at the classrooms

For this Project, 10 Government High Schools and 1 observation home have been identified for installation of 15 Smart Classrooms as provided in the table below.

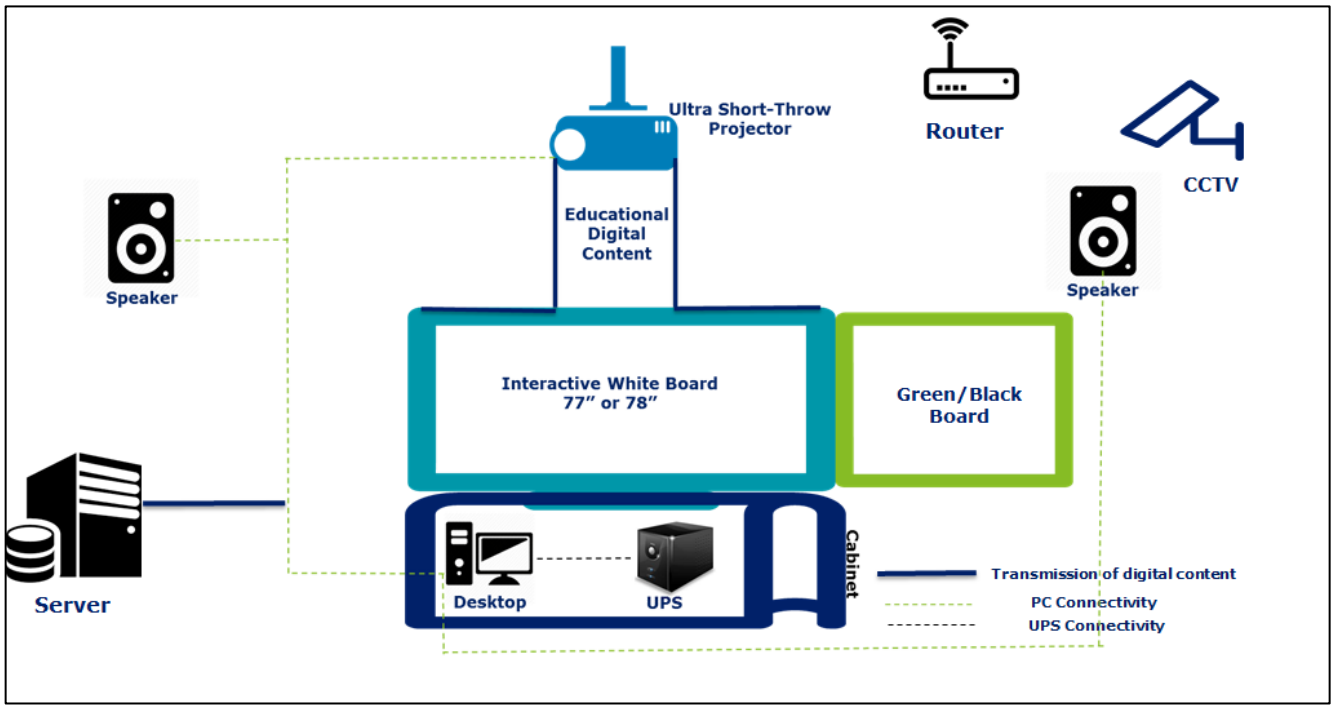
No.	Name of School	Number of Smart Classroom
1	Municipal high school, Panposh	2
2	Developed Area high school, Civil township	1
3	Guru Nanak Khalsa School	2

[6] Source: Census 2011
[7] Source: Block Education Office, Rourkela
[8] Source: Block Education Office, Rourkela

No.	Name of School	Number of Smart Classroom
4	Rashtriya Vidyalaya high school, Near Railway Station	1
5	Kalyani Devi Nodal, Sibaji Marg	1
6	Uditnagar high school, Uditnagar	2
7	Government Girls high school, Uditnagar	1
8	Town Nodal, Daily Market	2
9	DAV high school, Bisra Road	1
10	Urdu High School, Nala Road	1
11	Observation Home	1

Indicative Solution Architecture

The Smart Classroom solution architecture will enable transmission of digital content from the centralized server housed at command and control centre to the individual classroom desktops which gets projected over the interactive whiteboard, with video feeds of the classroom being transmitted to Command Centre for surveillance purpose. A high level schematic diagram of the proposed solution is depicted below:



Minimum Functional Requirements

S. No.	Minimum Functional Requirement	Compliant (Yes / No)
1. Hardware system requirements for Smart Classrooms		
SCR/FR/1.1	Smart Classrooms shall be equipped with Projectors, Audio Systems, Digital Smart Board and CCTV surveillance system	
SCR/FR/1.2	CCTV surveillance system shall be integrated with the ICCC with its video feeds recorded and available for viewing on demand on the video wall to monitor functioning of the smart classrooms by concerned authorities	
SCR/FR/1.3	Provision for dedicated server to store the educational contents	

S. No.	Minimum Functional Requirement	Compliant (Yes / No)
SCR/FR/1.4	Server will be placed at command center and will be wirelessly connected to all the smart classroom's desktop for access to the educational content	
2. Institutional requirements for enabling Smart Classrooms		
SCR/FR/2.1	The teachers are required to be trained on the digital course modules, operating the system and delivery of lectures with the help of interactive media. Training shall be imparted during inception stage and shall be followed by refresher trainings as and when required.	
SCR/FR/2.2	A minimum of two teachers per smart class are to be trained.	
3. Support System for Smart Classrooms		
SCR/FR/3.1	Support Manual (to include Installation academic content, Administration Manual and operational, instructional User Reference etc.) in English/Hindi/Odiya/Urdu	
SCR/FR/3.2	The hardware components shall be operative on "plug and play" basis, without the need of any proprietary license.	
SCR/FR/3.3	There should be proper security features to protect the system from misuse within the class and online.	
SCR/FR/3.4	Provision for installation of e-studio as per future requirement in one classroom	

Minimum Technical Requirements

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
1. Desktop Computers For Class Rooms/Resource Room		
SCR/TR/1.1	The workstations shall have a wireless optical mouse with USB connection complying with FCC and CE norms.	
SCR/TR/1.2	The workstation shall be Energy star 5.0/BEE star certified.	
SCR/TR/1.3	The workstations shall have a 107 Quiet Key English wireless keyboard with USB connection.	
SCR/TR/1.4	Workstation shall have a standard audio sound card and speakers.	
SCR/TR/1.5	The workstations shall have an Intel Core i7 4th Generation, quad core processor with 3.40 GHz or better.	
SCR/TR/1.6	The workstations shall have at least 8 GB DDR3 memory @ 1600 MHz.	
SCR/TR/1.7	The workstations shall have a min. of 4 DIMM slots supporting up to 32GB ECC. One DIMM Slot must be free for future upgrade.	
SCR/TR/1.8	The workstations shall have a min. 1 TB SATA III hard disk @ 7200 RPM or higher.	
SCR/TR/1.9	The workstations shall have shall a colour LED monitor of minimum 21" diagonal non-glare screen and a dual AMD Radeon HD 7470 full height video adapter with VGA, DVI, and HDMI ports or better.	
SCR/TR/1.10	The graphics card shall have a minimum resolution of 2560 x 1440 with 5ms response time or better specifications.	
SCR/TR/1.11	The workstations shall have a DVD multi burner and Dual Layer DVD-RW as an internal optical drive or better.	
SCR/TR/1.12	The workstations shall have an industry-standard professional-grade operating system. Acceptable systems include Microsoft Windows 8 or better.	
SCR/TR/1.13	The workstations shall have at the minimum ports: 1 serial, 6 USB 2.0 or higher with 2 in the front, integrated autosensing RJ-45 network interface, and Line-In/Mic In and Line-out/speaker Out (3.5 mm) audio in/out jacks.	
SCR/TR/1.14	The workstations shall have an expansion bus of 3 PCI Slots; 4 ISA Slots (3 slot shared).	
SCR/TR/1.15	The workstations shall have Microsoft Office Professional and Antivirus.	
SCR/TR/1.16	Other pre-loaded software (open source/ free) shall be Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
SCR/TR/1.17	The AC input power shall be 230 VAC +/- 10% at 50/60 Hz +/- 1Hz.	
SCR/TR/1.18	The workstations shall have a dual port 1 Gbps Ethernet network interface card.	
SCR/TR/1.19	The workstation shall be operational in temperature as per City requirement	
SCR/TR/1.20	The workstation shall be loaded with advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server.	
2. Networking Specification		
SCR/TR/2.1	24 Port Smart Switch with loop back detection, 24 x 1 CAT6 Patch Panel, RJ-45 connector, I/O box, Necessary electrical items and cables to connect and access device/terminal to desktop computer as per requirement.	
3. Metallic Cabinet/Podium/other arrangement		
SCR/TR/3.1	Podium with lockable housing facility for the keep and safety of the desktop/ CPU /UPS /Keyboard /Mouse/remote/stylus. The entire system shall be placed in a single cabinet with floor bearing and floor supported to keep it strong and stable. The tray for the keyboard and mouse is placed high enough for the teachers to reach in ease. The cabinet shall be such that all hardware is placed in it with hidden speaker system and concealed wiring	
4. Interactive White Board/White Board With Interactive Device/White Board With Interactive Projector (With Mounting Kit)		
SCR/TR/4.1	Active Size: Minimum 77/78” diagonal or above	
SCR/TR/4.2	Technology: Infrared or latest technology*	
SCR/TR/4.3	Board surface: Scratch resistant, Solid surface ; maintenance free, Compatible with ink marker, any object touch	
SCR/TR/4.4	Aspect Ratio: 4:3 or 16:9 or 16:10	
SCR/TR/4.5	Writing Tools: Pen/ stylus/ finger	
SCR/TR/4.6	Active Area: Minimum active diagonal length of 2000 mm	
SCR/TR/4.7	Resolution: 8000*8000	
SCR/TR/4.8	Operating system compatibility: Compatible with Windows XP or higher operating system and compatibility with Linux Operating System*	
SCR/TR/4.9	Computer Interface: Standard one USB	
SCR/TR/4.10	Power: Through USB Port*	
SCR/TR/4.11	Annotation software: Annotation software shall include features like draw, pens, annotate, erase, colour, shapes, sizes, text, edit, fonts, stamp, move, capture picture, video, save, rotate, undo, image gallery, print, floating key- board and background etc.*	
5. Projector System (Ultra Short Throw Projector)		
SCR/TR/5.1	Projection System: DLP	
SCR/TR/5.2	Native Resolution: WXGA(1280X800)	
SCR/TR/5.3	Brightness: 2700 AL or higher	
SCR/TR/5.4	Contrast Ratio: 10000:1	
SCR/TR/5.5	Aspect Ratio: 4:3, 16:9, 16:10 and other prominent Aspect Ratios	
SCR/TR/5.6	Lamp Life(Normal/Economic Mode): 3500/5000 Hrs.	
SCR/TR/5.7	Remote Control: Full Function remote control unit for projector (To be supplied along with the projector)	
SCR/TR/5.8	Video compatibility: PAL, SECAM, NTSC, HDTV, DTV	
SCR/TR/5.9	Wireless Connectivity, storage and LAN: Multimedia Projector with wireless connectivity between PC and Projector, Storage media port and wireless LAN connectivity	
6. Audio System		
SCR/TR/6.1	4.1 Digital Surround system (wall mounted)	
7. Server		
SCR/TR/7.1	Servers will be provided to support local processing and storage as per the solution proposed by the Bidder and as per the Smart Classroom Project	
SCR/TR/7.2	A sufficient number of physical servers shall be provisioned such that their CPU, RAM, and other key server component performance do not individually exceed 50%	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
	utilization individually.	
SCR/TR/7.3	The MSI shall provision sufficient amount of storage to support the operational needs.	
SCR/TR/7.4	The server shall have Dual Core Processor Intel Xeon E5 Series or better.	
SCR/TR/7.5	The server shall have 16 GB of RAM and 5 TB of storage as a minimum. The memory shall be scalable to double the capacity configured.	
SCR/TR/7.6	The Server shall include hard drives based on volume of data to be stored. The transaction data storage requirements shall be estimated based on total transactions & related calculations as per the functional requirements.	
SCR/TR/7.7	The server shall have 2 processors with each having a minimum of 6 cores per processor.	
SCR/TR/7.8	The server shall include a Network Controller, 2 Gigabit Server Adapters with TCP/IP Offload Engine one standalone and one embedded on the motherboard.	
SCR/TR/7.9	The Server shall include (4) PCI-Express x4 or (2) PCIe interfaces 64- Bit/133MHz.	
SCR/TR/7.10	The Server shall include at least 5 - USB 2.0 or higher (preferable) compatible ports.	
SCR/TR/7.11	The Server shall include 2-Hot plug redundant power supplies and cooling fans.	
SCR/TR/7.12	The Server shall have an Optical Drive 48x SATA CDRW/DVD Combo Drive internal or external	
SCR/TR/7.13	The Server shall include 1 Serial port and 1 VGA (+1 front VGA on rack models).	
SCR/TR/7.14	The Server chassis shall be rack mountable and include rack mounting hardware.	
SCR/TR/7.15	The Server shall include a RAID 5 storage controller supporting up to (8) hot-plug Serial-attached SCSI (SAS) drives.	
SCR/TR/7.16	The Operating System shall be Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system.	
SCR/TR/7.17	Suitable commercial off-the-shelf antivirus software shall be provided for the duration of the contract.	
SCR/TR/7.18	The central system server shall have a hot standby to mitigate any risk of failure in central system which halts the system performance.	
SCR/TR/7.19	Server shall be designed to provide a fully redundant and fault tolerant system and shall be available for 99.99% or greater. The unscheduled down time shall be less than 0.01%.	
SCR/TR/7.20	Server shall be provided with the server load balancers and link load balancers as needed to optimize the overall IT infrastructure operations.	
8. UPS		
SCR/TR/8.1	1 KVA, Internal double battery	
SCR/TR/8.2	Backup of 10-15 minute	
SCR/TR/8.3	Input voltage of 160- 280V	
9. CCTV – Fixed Camera		
SCR/TR/9.1	The camera control shall comply with the latest release of Open Network Video Interface Forum (ONVIF) standards.	
SCR/TR/9.2	The camera shall include an integral receiver/driver. The receiver/driver shall be capable of controlling pan-tilt, zoom and focus locally and remotely from the ICCC.	
SCR/TR/9.3	The camera shall incorporate AGC circuitry to provide for compensation at low light levels.	
SCR/TR/9.4	The lens shall be integrated with the camera.	
SCR/TR/9.5	Video output resolution shall not be less than 1920x1080 pixels.	
SCR/TR/9.6	The camera shall be capable to produce minimum 30 frames per second (fps).	
SCR/TR/9.7	The camera shall provide automatic white balance, automatic exposure, automatic gain control, electronic shutter, and backlight compensation.	
SCR/TR/9.8	The camera shall be a true day/night cameras with mechanical IR cut filter.	
SCR/TR/9.9	The camera shall be capable of providing a high contrast colour picture with a full video output at a minimum illumination as mentioned in the specifications.	
SCR/TR/9.10	All cameras shall capture high definition video, compress the video using H.264, H.265 technique and transmit real-time using fibre optic based communications system.	
SCR/TR/9.11	The cameras shall capture audio and compress using G.711 technique and transmit real-time using fibre optic based communications system.	

S. No.	Minimum Technical Requirement	Compliant (Yes / No)
SCR/TR/9.12	All cameras shall support on-board real-time video content analysis.	
SCR/TR/9.13	All cameras shall support both Constant Bit-Rate (CBR) and Variable Bit- Rate (VBR) options.	
SCR/TR/9.14	The camera shall support up to 2 video profiles, each providing independent configuration of bitrate, framerate and resolution.	
SCR/TR/9.15	The camera shall support video compression up to 6Mbps.	
SCR/TR/9.16	The camera shall support audio compression using the G.711 compression	
SCR/TR/9.17	The camera shall support on-board storage via micro SDHC slot and card with a minimum capacity of 64 GB.	
SCR/TR/9.18	All cameras shall have integral in-built or external adaptive IR technology. For fixed cameras, the IR shall support a range of at least 30m	
SCR/TR/9.19	For Fixed Cameras: - The fixed camera shall provide a minimum focal length range of 3- 10 mm compensated with digital zoom and shall be remotely controllable from the camera control transmitter at ICCC. - The fixed camera shall capture video using 1/3” progressive scan CMOS or better. - Fixed Camera resolution shall be 1920 x 1080 or better.	
SCR/TR/9.20	There shall be a minimum of 100 assignable automatic preset positions.	
SCR/TR/9.21	There shall be a minimum of 8 definable privacy zones.	
SCR/TR/9.22	All cameras shall provide effective 24/7 imaging performance for CCTV surveillance applications.	
SCR/TR/9.23	All cameras shall provide user control, with remote configuration for functions including streaming and compression settings, exposure, white balance, flicker control, picture size, cropping/privacy, brightness, sharpness, saturation, day-night switching point, frame rate, image rotation, snapshot, dynamic bandwidth allocation and motion detection.	

Artificial Intelligence , Machine Learning and Edge Analytics

Objective

For all sensor data collection and analytics, RSCL intends to leverage Artificial Intelligence (AI) and Deep Learning technology to analyze the huge amount of metadata, live feed coming from multiple sensors across several locations in the city. All use cases should be able to run leveraging artificial intelligence on all the Camera feed with minimum 80% accuracy to be achieved and should show continuous improvement during operations and maintenance in every 3 months (quarterly). Minimum 10 uses cases shall be running on each camera feed at any point of time on DC for Surveillance, ITMS SWM, Municipal use case etc.

Responsibility of MSI

The functional requirements and technical specifications provided in this RFP are indicative and providing guiding rules. The MSI is free to offer products and solutions, which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The MSI is encouraged to design an optimal solution, which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The MSI is fully responsible for the specified outcome to be achieved using artificial intelligence technology.

MSI should propose solution, which is implemented in minimum 5 projects and 3 to 4 different use cases mentioned below based on AI across the world. Evidence to be submitted for project executed.

Minimum Functional Requirements

Following illustrative use cases to be implemented using AI based video analytics by the CCTV cameras/sensors and continuous learning capability through Artificial Intelligence.

S.No.	Component	Specifications	Compliant (Yes / No)
AIML/FR/1.1	AI based Video Analytics System Use cases	These use cases are to be implemented using Artificial Intelligence through various cameras, sensors implemented in the field (Field device agnostic) implemented by RSCL with continuous learning capabilities at Data Centre.	
		• Graffiti and Vandalism detection, Defacing/Destroying the public property and street furniture.	
		• Debris and Garbage detection	
		• Attendance of sanitation workers on site by face recognition	
		• Sweeping and cleaning of streets/bins before and after	
		• Garbage bin, cleaned or not	
		• Identification of Garbage carrying tractor trailers which are not closed/covered as per municipal standard	
		• Identification of vehicles carrying the construction materials and building demolish materials	
		• Litter detection	
		• Tracking of garbage truck movement and Quantity of garbage dumped at dumpsite	
		• Detection and Recognize the pattern of demonstration and conflicts in crowd	
		• Detection and classification of human, animal and vehicle	

S.No.	Component	Specifications	Compliant (Yes / No)
		• Applicable Safety and Surveillance related used cases (as detailed in Safety/FR/ 1 to Safety/ FR/7) including but not limited to: - Behavioural Biometry : Identification through multiple behaviour - Parking violation - Speeding vehicle - Accident detection - Loitering detection - Person climbing barricade - Person collapsing - Person/Face recognition - Gesture recognition : Identification through gesture change	
		• Vehicle of interest' tracking by colour, speed, number plate	
		• Helmet detection on two wheeler	
		• Unwanted/ banned vehicle detection	
		• Wrong way or illegal turn detection	
		• Public toilet cleaning and number of people using public toilets	
		• Environmental condition detection	
		• Fire detection at minimum 50 plus high risk locations.	
		• Monitoring of under bridge Storm water logging.	

Minimum Technical Requirements

S.No.	Component	Specifications	Compliant (Yes / No)
AIML/TR/1.1	AI based Video Analytics System	• Deliver min 5.5 teraFLOPS of FP16 performance or better	
		• Support Wi-Fi, Bluetooth, 3G/LTE connectivity options	
		• Should have 100Mb/1GbE management network link for data transfer	
		• Support Min 1GbE (via RJ45) or 10GbE (SFP+) or better	
		• Have operating temperature range as per City requirement to withstand outdoor operating environment as per city conditions	
		• System should have minimum power consumption.	
AIML/TR/1.2	AI with Continuous Learning & Improvement system	• Deliver processing units' performance of 1 petaFLOPS on FP16 or better	
		• Have software tools for achieving the following tasks- Resource allocation, queueing of jobs, performance monitoring and creating software containers	
		• Support commonly used Deep Learning based AI frameworks like TensorFlow, CNTK etc.	
		• Have minimum 512 GB system memory per system or better	

S.No.	Component	Specifications	Compliant (Yes / No)
		• Have dual 10GbE and 4 IB EDR per system.	
		• Min power consumption per system.	
		• Have dual 20-core Intel Xeon E5-2698 or better per system.	
		• Support parallel computing architecture.	
		• Support software libraries for continuous learning and improvement for betterment of intelligent video analytics software installed in edge/field devices using Deep Learning based AI methodologies.	

Implementation Schedule and Payment Terms

Project Implementation Schedule

MSI shall deliver all project activities/milestones/deliverables to the Client as per the timelines stated in this section. Client or its authorized representative shall take thirty (30) days to review and provide comments on all respective deliverables. MSI shall ensure that all comments provided by the Client or its authorized representative shall be incorporated in the final version of all deliverables.

All deliverables indicated in the tables below are indicative only and shall be read in conjunction with the Scope of Work section and Standard Form of Contract of the RFP for detailed requirements. Client or its authorized representative reserves the right to ask for additional information, documents and deliverables throughout the Project.

The proposed implementation schedule for the project is indicated below:

S. No.	Milestone	Deliverables	Timelines (in Months)
1.	**Project Implementation Phase** (T = Date of Signing of Master Service Agreement)		**T+12 Months**
Phase I			**T + 6 Months**
1.1	**Project Inception Report**	Detailed site survey report including infrastructure requirement analysis, hardware deployment plan, recommended action plan to address the gaps, budget estimates for addressing the gaps uncovered during the survey, phase wise location distribution etc. Detailed Project Plan including resource deployment, Communication plan, Risk management plan, Information Security and Business Continuity, Sensitization & Training Plan, Operations management plan etc.	**T + 1 Month**
1.2	**Requirement Study** • Integrated Command and Control Centre (ICCC) including Data Centre • City IT Network Infrastructure • Intelligent Waste Management System (IWMS) • Intelligent Traffic Management System (ITMS) • Safety and Surveillance • City Governance Services including City Web Portal & Mobile App • City Wi-Fi • Environmental Monitoring System • Variable Message Signboards (VaMS) and Public Address System (PAS) • Smart Classrooms • Enterprise GIS • Integration of Smart City Platform with AI and Edge Analytics	Architecture and design for ICCC, City IT Network and Data Centre including Data Centre Architecture, Network Architecture, Security architecture etc. Submission of FRS, SRS including Solution Architecture, Application Design Documents of the proposed system Integration report for external applications	**T + 3 Months**

S. No.	Milestone	Deliverables	Timelines (in Months)
1.3	**Quick-Wins at select locations on a pilot basis**	• Safety and Surveillance System • Traffic Signals • City Wi-Fi • Mobile Application	**T + 3 Months**
1.4	**Phase I: Go Live** **Supply, installation, commissioning, training & operationalization of the following modules** • City IT Network Infrastructure • Adaptive Traffic Signal Control System • Safety and Surveillance System • City Web Portal • City Wi-Fi • VaMS and PAS • Temporary ICCC and temporary Data Centre	• Site Completion/readiness Report • Delivery Acceptance Reports from RSCL/authorized entity • Installation & Commissioning Reports • Software Licenses details • UAT/FAT and Go Live Certificate from RSCL/authorized entity • Training Content & Completion Certificate • Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	**T + 6 Months**
Phase II			**T + 9 Months**
1.4	**Phase II: Go Live** **Supply, installation, commissioning, training & operationalization of the following modules** • Intelligent Waste Management System • Traffic Violation Detection System • Environmental Monitoring System • Smart Classroom	• Site Completion/readiness Report • Delivery Acceptance Reports from RSCL/authorized entity • Installation & Commissioning Reports • Software Licenses details • UAT/FAT and Go Live Certificate from RSCL/authorized entity • Training Content & Completion Certificate • Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	**T + 9 Months**
Phase III			**T+12 Months**
1.5	**Phase III: Integration and Project Final Go Live** Integration with external applications (existing & proposed) with ICCC and DC **Supply, installation, commissioning, training & operationalization of the following modules** • Migration of temporary Integrated Command and Control Centre (ICCC) including Data Centre to permanent location • City Governance Services and Mobile App • Enterprise GIS • Integration of Smart City Platform with AI and Edge Analytics	• Site Completion/readiness Report • Delivery Acceptance Reports from RSCL/authorized entity • Installation & Commissioning Reports • Software Licenses details • UAT/FAT and Go Live Certificate from RSCL/authorized entity • Training Content & Completion Certificate • Security Audit Certificate from Cert-In/STQC for Data Centre and Applications • Source code of portal, Mobile App & customized applications	**T + 12 Months**
2.	**Project Operation and Maintenance Phase** (T1 = Date of Final Go Live)		**T1+60 Months**
2.1	**Operation and Maintenance**	• Monthly & Quarterly SLA Reports • Adhoc Reports	T1 + 60 Months

Project Payment Schedule

MSI should complete all the activities within the defined timelines as indicated above. The timeline will be reviewed regularly during implementation phase and may be extended in case RSCL feels that extension in a particular Request Order/Integration or any track is imperative, for the reason beyond the control of the bidder. In all such cases RSCL's decision shall be final and binding. MSI will be eligible for the payment based on the completion of activities and approval of the relevant deliverables.

The proposed payment schedule for the project is indicated below

S. No.	Milestones	Timelines	Payment
1.	Project Inception Report	T + 1 Month	1% of CAPEX
2.	Requirement Study	T + 3 Months	2% of CAPEX
3.	Hardware Delivery & commissioning of Temporary ICCC & DC	T + 5 Months	3% of CAPEX
4.	Phase I: Go Live	T + 6 Months	24% of CAPEX
5.	Phase II: Go Live	T + 9 Months	10% of CAPEX
6.	Phase III: Integration and Project Final Go Live	T + 12 Months	30% of CAPEX
7.	One year of successful completion of Project Final Go-Live	T1 + 12 Months	30% of CAPEX shall be paid in two (2) equal half yearly instalments
8.	Project Operations & Maintenance phase for a period of 60 months from the date of Final Go Live	T1 + 60 Months	OPEX will be paid in twenty (20) equal quarterly instalments spread across 5 years Post Final Go-Live

Note 1:

If successful bidder requests for Mobilization advance, following conditions shall be applicable

- Mobilization advance can be maximum of 10% of capex value
- Mobilization advance shall be released only after receipt of Bank Guarantee of 110% of the requested amount
- Mobilization advance shall be interest bearing and PLR rate of interest shall be payable to RSCL by the successful bidder
- Mobilization advance shall be adjusted by Phase III of project implementation (T + 12 months)

Note 2:

- All payments to the Systems Integrator shall be made upon submission of invoices along with necessary approval certificates from RSCL
- The above payments are subject to meeting of SLA's failing which the appropriate deductions as mentioned in the Volume III of this RFP

Project Governance

The proposed project governance structure would comprise the following:

- High level steering committee, comprising the Chairman, MD, select Board members of RSCL and the MSI Project Director
- Project specific working group, comprising the respective functional leads (for example, SP (Traffic) for ITMS), the MSI Project Manager and select team members for the respective module(s)
- Core team members, domain specialists and designated counterpart staff from RSCL/ concerned Government Agency for individual modules

- Support team

The steering committee would meet once every month to take important decisions and approve any strategic decisions to ensure timely implementation and address identified bottlenecks. The project specific working groups would convene on a weekly or a bi-weekly basis to discuss progress and address any issues pertaining to implementation.

Annexure: Standards and Guidelines

Annexure A: Guiding Principle for Smart City Solutions Development

The proposed Smart City Solutions should be designed and implemented keeping the following principles (Indicative):

a. **Transformational Nature of Smart City applications** - Applications should look to fully embrace mobile adoption, online authentication, etc. to transform the processes completely and offer wider choice and no/low touch point for residents to interact directly. It is critical that project design are aligned to larger trends and designed for next decade rather than past.

b. **Use Of Open Standard for evolving Technology :**The entire system would be built to be open (standards, open API, plug-n-play capabilities like virtual environments, creating sandbox), components coupled loosely to allow changes in sub- system level without affecting other parts, architected to work completely within a heterogeneous compute, storage, and multi-vendor environment. Use of the latest & best available standards to avoid locking in obsolescent technologies simulated services environment can help agencies to save cost, Infrastructure and time in testing multiple application integrations. Large integrated systems of Smart City operations should be designed to get best cost and performance advantages of natural technology curve (constant increase of speed and decrease of cost), architecture should be open and vendor neutral, and designed for horizontal scale.

c. **Distributed, PKI based Authentication and Authorization -** The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.

d. **Security and privacy of data** – The security services will cover the user profile management, authentication and authorization aspects of security control. This service run across all the layers since service components from different layers will interact with the security components. All public contents should be made available to all users without authentication. The service will authenticate users and allows access to other features of the envisaged application for which the user is entitled to. The system should be designed to provide the appropriate security levels commiserate with the domain of operation. Also the system will ensure data confidentiality and data integrity. The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be blocked and well supported (and implemented) with the security policy (In line with Govt of India Security and Privacy data policy, AP Govt security and privacy of data policy and RSCL's security and Privacy of data policy). The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. The security and privacy of data is applicable for all the systems that are in scope of this RFP (Including end field devices, Mobile phones, Tablets etc..,).

   There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users.

   Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. The authority would carry out the security audit of the entire system upon handover and also at regular interval during O&M period. MSI's solution shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development). All the applications shall be test cleared by MSI through STQC certification as fit for use and safe to use in Government networks and systems.

Field equipment installed through this Project would become an important public asset. During the contract period of the Project the MSI shall be required to repair / replace any equipment if stolen / damaged/faulty with same / equivalent / better equipment and at the end of the contract period shall transfer all systems and equipment in working condition to the RSCL. Appropriate insurance cover must be provided to all the equipment's supplied under this project.

- The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below.
- The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.
- The solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.
- Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and disaster recovery system.
- The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.
- The overarching requirement is the need to comply with ISO 27001 standards of security.
- The application design and development should comply with OWASP top 10 principles
- A secure solution should be provided at the hardware infrastructure level, software level, and access level.
- Authentication, Authorization & Access Control: 3 factors (User ID & Password, Biometric, and Digital Signature) security mechanisms should be implemented to enable secure login and authorized access to portal information and services.
- Encryption Confidentiality of sensitive information and data of users and portal information should be ensured.
- Appropriate mechanisms, protocols, and algorithms necessary to protect sensitive and confirmation data and information both during communication and storage should be implemented.
- Data security policies and standards to be used as per government of India guideline.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level. Database design must consider and incorporate data integrity requirements.
- Role based access for all the stake holders to be implemented to access and use the system
- Ability to adopt other authentication mechanism such as Electronic Signature Certificates
- Authorization validity to be ensured for the users providing the Data to the system. Data should be accepted only from the entity authorized
- Audit trails and Audit logging mechanism to be built in the system to ensure that user action can be established and can investigated if any can be aided(e.g. Logging of IP Address etc.)
- Data alterations etc. through unauthorized channel should be prevented.
- Industry good practice for coding of application so as to ensure sustenance to the Application Vulnerability Assessment
- Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
- Access controls must be provided to ensure that the system is not tampered or modified by the system operators.
- The security of the field devices must be ensured with system architecture designed in a way to secure the field devices in terms of physical damage & unauthorized access.
- The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Center (DC) should talk to the applications hosted in the data center through predefined APIs only.

- APIs should be published and the IT systems be running on standard protocols like JSON / XML or REST etc.
- From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems.
- All IoT sensors deployed as part of Smart cities system should communicate only to the authorized wired/wireless network, and do not hook on to the rogue networks. The guidelines to secure Wi-Fi networks as published by Department of Telecom must be followed.
- Wireless layer of the Smart City Network should be segmented for public and utility networks by using Virtual Private Networks (VPNS) or separate networks in the wired core, so that any traffic from the internet users is not routed into the sensor networks and vice-versa.
- All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in transit must be encrypted
- Authentication of sensors in the Smart city should happen at the time of provisioning the sensors, and adding them into the system, and should be based on physical characteristics of the sensors like MAC lD, Device lD etc.
- All the sensors deployed across city as part of this RFP should be regularly calibrated to ensure correctness in readings.
- Sensors deployed in solutions to set up Smart city should be hardened devices with the ability to be upgraded remotely for firmware through encrypted image files.
- The Sensors or edge device deployed in Smart city should not have any physical interface for administration. Monitoring of systems and networks should be undertaken remotely.
- All the sensors in the Smart city should connect to a completely separate network.
- As various sensors use multiple protocols to communicate with the underlying network with varied security capability, the system should allow provisioning necessary authentication and encryption at the gateway or the nearest data aggregation level if the sensor is not able to do the same.
- Secured Information and Event Management system monitoring all Smart City networks, devices and sensors to identify malicious traffic Activities such as anti-spoofing (no one should be able to masquerade for inappropriate access), anti-sniffing (no one should be able get data and interpret it), anti-tampering (no one should be able to put/change data which was not meant to be put/changed) should be taken care for data in transit, as well as data at rest, from internal and external threats.
- More detailed guideline published by MOUD can be found at http://mohua.gov.in/pdf/58fd92b5545b85821b621a862dCyber_Securitypdf.pdf

e. **Sustainable & Scalable Solution-** Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system imposed restrictions on the upward scalability in number of cameras, data centre equipment's or other smart city components. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure).

The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The

expectation is that the system should sustain at least 10 years from GO-Live. There must not be any system imposed restrictions on the upward scalability in number of field devices.

f. **Availability -** Components of the architecture must provide redundancy and ensure that are no single point of failures in the key project components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data center components level and offering system High Availability and failover. The solution should Meet the minimum of following availability requirements
   - Load Balanced across two or more Web Server avoiding single point of failure
   - Deployment of multiple application instances should be possible
   - Distributed or load balanced implementation of application to ensure that availability of services is not compromised at any failure instance.
   - Provide analytic tools build into the system that shall support automatic detection of Anomalies and their quick mitigation.

g. **Manageability -** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the scalability of the system.

h. **Interoperability** - Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:
   - at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and
   - Be of leading industry standards.

i. **Convergence -** RSCL has already initiated many projects which have state of the art infrastructure at field locations deployed under them. The ITMS Infrastructure should be made scalable for future convergence needs. Under the smart city program, RSCL has envisaged to create a state of the art infrastructure and services for the citizens of RSCL, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. Equipment like Junction Boxes and poles deployed under the ITMS project at the field locations will be utilized to accommodate field equipment's created under the other projects of RSCL. The procedure for utilization of the infrastructure will be mutually agreed between the RSCL and MSI

j. **Application Architecture-** The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors. The standards should (a) at least comply with the Published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry.

The modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system/ application to avoid any kind of irregularities within the system by any User / Application.

MSI shall design and develop the Smart City System as per the Functional and System requirement specifications finalized.

Cyber Security-

As per the letter issued by National Security Council Secretarial, New Delhi, it is mandated to follow norms and regulations of Cyber Security for Smart City Model Framework. A MSI must provide compliance to each of the below mentioned points:

- The generic architecture of smart city generally consists of four layers- a sensing layer a communication layer a data layer and application layer, and these four layers are overseen by the smart city security system, Architecture of information Technology systems deployed in Smart city need to be open interoperable and scalable.
- The reference architecture of information Technology (IT) infrastructure in Smart city suggested by National Institute of Standards and Technology (NIST) serves as a common starting point for system planning while promoting interoperable functional building blocks, which are required in a smart city.
- The message exchange between various applications in the smart city should be fully encrypted and authenticated. Any application outside the Data Center (DC) should talk to the application hosted in the datacenter through only predefined APIs.
- While it is necessary to converge multiple infrastructure into one Central platform for ease of management it is mandatory that such applications hosted in the central data centre support tenancy with adequate authentication and role based access control mechanism for each tenant pertaining to their respective infrastructure.
- In multi-tenant architecture there should be provision for flow of normalized data only to respective tenant partition (s) in a predefined manner with adequate authentication and encryption mechanism.
- The Smart city architecture should be capable of managing heterogeneous data which would be continuously communicated through numbers devices following different protocols, in order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow.
- Between applications and back end system, HTTP, SQL , FTP, SNMP, SOAP, XML, SSH, SMTP, Between back end systems and field devices message Queue Telemetry Transport (MQTT)XMPP, RESTful HTTP Constrained Applications protocol (CoAP) SNMP , IPV4/6, BACent LON works Low power Wide Area Network (Lora) Fixed, 4G/5G Wi-fi Wimax, 2G/3G from field devices, Zigbee Olp , ETSI LTN IPv4/6,6 LowPAN ModBus Wi-fi-802, 15.4 enOCean LoRA, RFID NFC Bluetooth, Dash7 Fixed ISM & Short range banks
- Data Layer (Termed as city Digital platform/fabric) should be capable of communicating with various types of sensors/ devise and their management platforms/applications for single /multiple services irrespective of software and application they support. Data exchange between various sensors and their management applications must strictly happen through this layer. Thus making it one true source of data abstraction, normalization correlation and enable further analysis on the same adequate security checks and mechanisms as described in later points to be deployed to protect data layer from data confidentiality Brach and unauthorized access.
- The entire information Technology (IT) infrastructure deployed as part of Smart city should follow standards like ISO- 27001, ISO- 22301, ISO 37120, ISO 3712, ISO 27017, ISO 27018, BSIS PASS 180 BSI PAS 181, BSI PAS 182 for Wi-Fi access – PEAP(Protected Extensible Authentication Protocol), 3rd Generation Partnership Project (3GSPP) Etc., As appropriate.
- Application Program intensifies (APIs) should be published and the IT System be running on standard protocols like JSON/XML or REST etc.
- From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords) the authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network.

And there is no rogue data that is sent to the control system to generate false alarms of sabotage the system.

- Wireless broadband plan and architecture for the specific city may be prepared detailing the existing fiber system and other supporting infrastructure so as appropriately interfacing another or citywide wireless network.
- All sensors deployed as part of IT and IT based system in the Smart Cities should communicate only to the authorized wireless network and do not hook on to the rogue networks the guidelines to secure Wi-Fi network as published by Department of Telecom must be followed
- Wireless layer of the Smart city Network should be segmented for public and utility networks by using virtual private networks (VPNs) or separate networks in the wired core so that any traffic from the internet users is not routed into the sensor networks and vice-versa.
- All traffic from the sensors in the Smart city to the application servers should be encrypted Secure Socket Layer (SSL) and authenticated prior to sending any information. The data at rest and in Transit must be encrypted.
- Authentication of sensors in the Smart City Should happen at the time provisioning the sensors and adding them into the system and should be based on physical characteristics' of the sensors like MAC ID, Device ID etc.
- Sensors deployed in solution to set up Smart City Should be hardened device with the ability to be upgraded remotely for firmware through encrypted image files.
- As various use multiple protocols to communicate with the underlying network with varied security capability the system allows provisioning necessary. Authentication and encryption sat the gateway or the nearest data aggregation level if the sensor is notable to do the same.
- The Sensors or edge device deployed in Smart city should not have any physical interface for administration Monitoring of system and networks should be undertaken remotely.
- The sensors deployed in Smart City should be of low power consumption and should work on self-sufficient power sources.
- All devices and system deployed in Smart City should be hardened and have the ability to be upgraded remotely for firmware through encrypted image files with authentication mechanism to complete the operation.
- All the sensors in the Smart city should connect to a completely separate network.
- The Data center should be segmented into multiple zones with each zone having a dedicated functionality e.g. all sensors for one operational domain can connect to the data center in one zone, and the internet facing side of the data center should be in another zone.
- The Internet facing part of the data center should have a Demilitarized zone where all the customers' application servers would be located that are customers facing. Only these serves can assess the data from the actual utility applications servers on predefined ports.
- The Customer application servers should be accessed only by the web server that in hosted in different zone of the data center.
- The following should be implemented in the data Center – Firewalls, Intrusion detection & intrusion prevention system , Web Application Firewalls, Behavioral Analysis system for anomaly detection, correlation engine, Denial of Service prevention device, Advanced persistent. Threat Notification mechanism, federated identity and access management system etc.
- Security information and Event Management (SIEM) monitoring on all smart city Networks devices and sensors to identify malicious traffic.
- All application and apps will undergo static and dynamic security testing before deployment and be tested with respect to security on regular bias at least once in a year.
- All applications and Apps deployed as part of Smart city be hosted in India.
- The said architecture provide Automatic and secure updates of software and firmware etc.
- All system and devices should provide auditing and logging capabilities.
- Ensure vendor Compliance to remove any backdoors, undocumented and hard cored accounts.

- End to End solution should be provided with annual end to end service availability of 99,999 percent. The end to end service agreement should be in place for minimum period of five years form the data or operation of the systems.
- Appropriate terms may be set up to monitor cyber incidents and mitigation of same.
- All the information on incidents be shared regularity with Indian computer Emergency response Team (CERT-in) and ICIIPC (National Critical information Infrastructure Protection Center) and take help to mitigate and recover from the incidents.

Annexure B: Disaster Management

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S.No	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, Risk management – Principles and guidelines	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 -Seismic Rehabilitation of Existing Buildings	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality, the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

Annexure C: Estimates of Data Migration and Transactions in the Existing E-Governance System

Sl. No.	Component	Total Records	Remarks
1	Property Information	16748	RMC - 16748
2	Street Light Poles	10855	RMC - 10855
3	Hoarding Information (Govt.)	149	RMC - 149
4	Hoarding Information (Private)	114	RMC - 114
5	Employee Records (Regular)	544	RMC – 486, RSCL-5, RDA-53
6	Employee Records (Contractual/Adhoc)	155	RMC - 148 (20 contractual , 128 NMR/ADHOC), RDA – 1, RSCL - 6 (contractual)
7	**Infra Assets**		
a.	Roads (KM)	473.43	RMC - 473.43 (around 300 kms of Road have been put on GIS Map)
b.	Drains (KM)	497.82	RMC - 497.82
c.	Vehicles	37	RMC – 35, RDA - 2
d.	Dustbins	100	RMC - 100
e.	Engineering Projects	134	RMC - 124 (Unnati - 117, AMRUT Parks - 1, PMAY - 1, Affordable Housing - 1, SBM Toilets - 1, Kalyan Mandap - 2, Panposh Market - 1) RDA - 10
8	**IT Assets (Nos.)**		
a.	Desktop	66	RMC – 50, RSCL-3, RDA-13
b.	Laptop	10	RMC – 3, RSCL-2, RDA-5
c.	UPS	69	RMC – 50, RSCL-4, RDA-15
d.	Mobile Phone Sets	32	RMC - 32
e.	CCTV Cameras	100	RMC - 100 (RMC Office - 64, Aahar Kendra - 24, Shelter for Urban Homeless - 12)
f.	Network Switches	7	RMC – 4, RSCL-3
g.	Wi-Fi Dongle	1	RSCL-1
h	Wi-Fi Access Point Devices	6	RMC – 4, RSCL-2
i	Printer	48	RMC – 45, RSCL-3