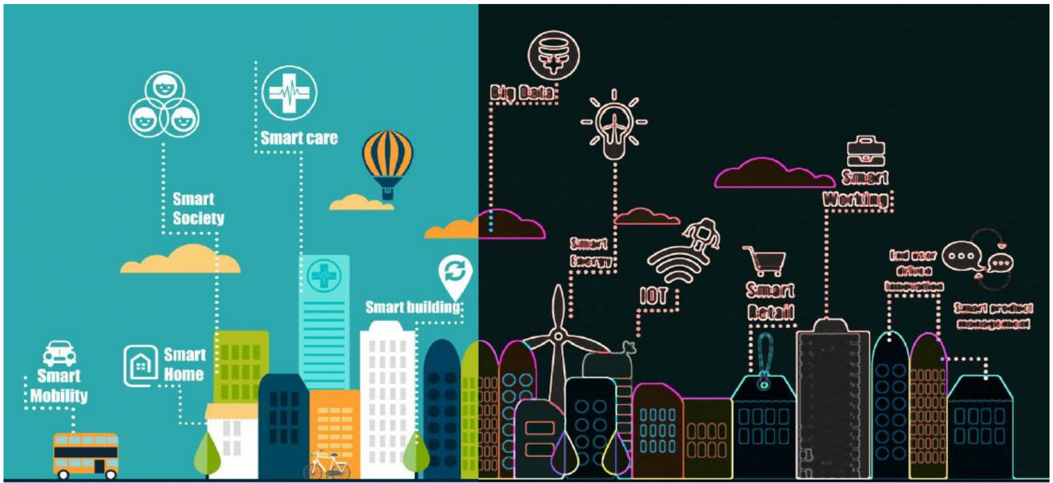
Kanpur Smart City

Request for Proposal

for

Master System Integrator for Implementation of Integrated Smart Solutions at Kanpur



Volume II: Scope of Work

Disclaimer

Kanpur Smart City Proposal (SCP) has been selected to implement the Area Based Development (ABD) and Pan-City proposals by Government of India (GoI) under Smart City Mission (SCM). KSCL SCP proposes served smart solution in ADB and cross pan-city providing various Smart feature/infrastructure.

To implement Smart City projects in KSCL, Kanpur Municipal Corporation and Uttar Pradesh Government has formed a SPV called Kanpur Smart City Ltd. (KSCL).

The KSCL has prepared this Request for Proposals (RFP) for Selection of Master System Integrator for Implementation of Command Control and Communication Centre for Kanpur City**"**. The RFP is a detailed document with specifies terms and conditions on which the bidder is expected to work. These terms and conditions are designed keeping in view the overall aim and objectives of the Command Control and Communication Centre. KSCL has taken due care in preparation of information contained herein and believes it to be accurate. However, neither KSCL or any of its authorities or agencies nor any of their respective officers employees, agents, or advisors gives any warranty or make any representations, express, or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it.

The information provided in this document is to assist the bidder(s) for preparing their proposals. However this information is not intended to be exhaustive, and interested parties are expected to make their own inquiries to supplement information in this document. The information is provided on the basis that it is non–binding on KSCL any of its authorities or agencies, or any of their respective officers, employees, agents, or advisors. Each bidder is advised to consider the RFP as per its understanding and capacity. The bidders are also advised to do appropriate examination, enquiry and scrutiny of all aspects mentioned in the RFP before bidding. Bidders are encouraged to take professional help of experts on financial, legal, technical, taxation, and any other matters / sectors appearing in the document or specified work. The bidders should go through the RFP in detail and bring to notice of KSCL any kind of error, misprint, inaccuracy, or omission.

KSCL reserves the right not to proceed with the project, to alter the timetable reflected in this document, or to change the process or procedure to be applied. It also reserves the right to decline to discuss the Project further with any party submitting a proposal. No reimbursement of cost of any type will be paid to persons, entities, or consortiums submitting a Proposal.

Definitions/Acronyms

Terms	Meanings
ABD	Area Based Development
AMC	Annual Maintenance Contract
ANPR	Automatic Number Plate Recognition
ATCS	Adaptive Traffic Control System
BOM	Bill of Material
CCTV	Closed Circuit Television
COTS	Commercial Off-The-Shelf
CSP	Cloud Service Provider
DC	Data Centre
DMS	Document Management System
DRC	Disaster Recovery Centre
ECB	Emergency Call Box
EMD	Earnest Money Deposit
FMS	Facility Management Services
GIS	Geographical Information System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GST	Goods and Services Tax
ICCC	Integrated Command and Control Centre
ICT	Information and Communication Technology
IP	Internet Protocol
IPF	Information Processing Facility
ISO	International Organization for Standardization
ISWM	Integrated Solid Waste Management
IT	Information Technology
ITDP	Institute for Transportation and Development Policy
ITMS	Intelligent Traffic Management System
LOA	Letter of Acceptance
MIS	Management Information System
MSI	Master System Integrator
NIT	Notice Inviting Tender
OEM	Original Equipment Manufacture

Terms	**Meanings**
OFC	Optical Fiber Cable
PA	Public Address
PoP	Point of Presence
PTZ	Pan Tilt Zoom
RFP	Request for Proposal
RACI	Responsible, Accountable, Confirm, Inform
RLVD	Red Light Violation Detection
KSCL	Kanpur Smart City Ltd.
SCM	Smart City Mission
SCP	Smart City Proposal
SDC	State Data Centre
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SPV	Special Purpose Vehicle
SVD	Speed Violation Detection
TCV	Total Contract Value
TDS	Tax Deducted at Source
TPA	Third Party Auditor
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
VAT	Value Added Tax
VM	Virtual Machine
VMS	Variable Message Sign

Table of Contents

1 Introduction 1
1.1 Project Objectives 1
1.2 Purpose of this RFP 1
2 Project Overview and Components 3
2.1 Components & Services Scope Overview 3
2.2 Component Architecture 5
3 Survey, Deign Consideration for finalization of detailed technical architecture and project plan 7
3.1 Commencement of Works 18
3.2 Existing Traffic Signal system 18
3.3 Road signs 18
3.4 Electrical works and power supply 18
3.5 Lightning-proof measures 18
3.6 Earthing System 18
3.7 Junction Box, Poles and Cantilever 19
3.8 Cabling Infrastructure 19
3.9 Integrated Command & Control Centre (ICCC) 20
3.10 Data Centre and Disaster Recovery Centre 21
4 Other Expectation and Consideration from MSI 22
4.1 Inception Phase 22
4.2 Requirement Phase 22
4.3 Design Phase 23
4.4 Development Phase 23
4.5 Integration Phase 25
4.6 Pilot Deployment 25
4.7 Go-Live Preparedness and Go-Live 26
4.8 Handholding and Training 26
4.9 Operations and Maintenance 29
4.9.1 Applications Support and Maintenance 29
4.9.2 ICT Infrastructure Support and Maintenance 31
4.9.3 Warranty support 31
4.9.4 Maintenance of ICT Infrastructure at the DC and ICCC 32
4.9.5 Compliance to SLA 38
4.10 Compliance to Standards & Certifications 38

4.11 Testing and Acceptance Criteria....39
4.12 Factory Testing....41
4.13 Final Acceptance Testing....41
5 Detailed Scope of Work....43
5.1 Scope of Implementation and Integration components:....43
5.1.1 Field Equipment: UPS and Others....43
5.1.2 Command Control & Communication Centre (ICCC / ICCC)....46
5.1.3 Smart City Data Centre....72
5.1.4 Network Backbone and Internet Connectivity....120
5.1.5 Smart Urban Solution....122
5.2 Scope of Integration:....210
5.2.1 Existing Solutions:....210
5.2.2 Future Solutions:....211
6 Project Governance and Change Management....211
6.1 Project Management and Governance....211
6.1.1 Project Management Office (PMO)....211
6.1.2 Helpdesk and Facilities Management Services....212
6.1.3 Steering Committee....212
6.1.4 Project Monitoring and Reporting....213
6.1.5 Risk and Issue management....213
6.1.6 Governance procedures....213
6.1.7 Planning and Scheduling....213
6.1.8 License Metering / Management....214
6.2 Manpower Deployment....214
6.3 Change Management & Control....215
6.3.1 Change Orders / Alterations / Variations....215
6.3.2 Change Order....216
6.4 Exit Management....217
6.4.1 Cooperation and Provision of Information....217
6.4.2 Confidential Information, Security and Data....217
6.4.3 Transfer of Certain Agreements....218
6.4.4 General Obligations of MSI....218
6.4.5 Exit Management Plan....218
7 Project Implementation Schedule, Deliverables and Payment Terms....219

7.1 Project Implementation Schedule and Deliverables Payment Schedule 219
7.2 Payment Schedule 223
8 Annexure: 223
8.1 Annexure I: Bill of Material 223
8.1.1 Pan City Network Backbone 223
8.1.2 Command Control and Communication Centre 224
8.1.3 Helpdesk 225
8.1.4 Data Centre 225
8.1.5 Data Recovery Centre 227
8.1.6 City Wi-Fi – Field Equipment 227
8.1.7 ITMS – Field Equipment 227
8.1.8 Smart Parking – Field Equipment 229
8.1.9 Environment Sensors – Field Equipment 229
8.2 Annexure II: ICCC Design Consideration 230
8.2.1 Key Design Considerations 230
8.2.2 Security 242
8.2.3 Software Development Lifecycle Continuous Build 246
8.2.4 Quality Assurance 247
8.2.5 Performance and Load Testing 247
8.3 Annexure III- Common guidelines regarding compliance of systems/equipment 249
8.4 Annexure IV- Tentative List of Locations 251
8.5 Annexure V: Standards 264

1 Introduction

1.1 Project Objectives

The key objective of this project is to establish a collaborative framework where input from different smart solutions implemented by KSCL, and other stakeholders can be assimilated and analysed on a single platform; consequently resulting in aggregated city level information. Further this aggregated city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens in coordinated and collaborative manner. Following are the key outcomes expected to be achieved by the proposed interventions:

a. Improved visualization of ambient or emergency situation in the city and facilitation of data driven decision making
b. Efficient traffic management
c. Enhanced safety and security
d. Better management of utilities and quantification of services
e. Asset Management
f. Disaster Management and Emergency Response
g. Efficiency improvement in public service delivery
h. Interdepartmental coordination and collaboration for faster execution of services
i. Implementation and Integration with all existing and future services as identified by Kanpur Smart City limited (KSCL) in the city including but not limited to (with provision for future scalability):
    - CCTV Surveillance System
    - Smart Lighting
    - Data Centre
    - Disaster Recovery Centre
    - Integrated Command and Control Centre
    - ICT Enabled Solid Waste Management
    - Intelligent Traffic Management System
    - E-Challan System
    - Public Bike Sharing
    - Smart Water Supply System
    - Smart Education
    - Smart Health Management System
    - Intelligent public transport Management
    - Smart pole
    - Smart Energy Management system

1.2 Purpose of this RFP

The purpose of this tender is for the Kanpur Smart City Limited (KSCL) to enter into a contract with a qualified firm for the Supply, Installation, configuration, Integration, Commissioning, Operations and Maintenance of integrated solutions to support the command, and control centre initiative for smart city initiative of KSCL. KSCL is looking to engage a Master Service Integrator -

- Who brings strong technology experience in smart city implementation, integration and operations through integrated and multi-agency coordination platform
- Who can develop Standard Operating Procedures for the various components of the project and link with uses cases prepared by them

- Who has a quality control plan in place to demonstrate that all equipment is tested and passed prior to shipping
- Who is capable of providing high quality installations of the project equipment
- Who is capable of maintaining and operating the complex smart city systems to provide maximum decision making support and performance of the systems
- Who brings forth expertise for traffic management, incident and emergency management
- Who has experience implementing city-wide ICT and surveillance system coupled with using the said systems efficiently through data analytics
- Who will strongly build capacity of various stakeholders for efficient operations and management of the proposed solutions

This tender is designed to provide interested bidders with sufficient basic information to submit proposals meeting minimum requirements, but is not intended to limit a proposal's content or exclude any relevant or essential data. Bidders are at liberty and are encouraged to expand upon the specifications to evidence superior bid understanding and service capability.

2 Project Overview and Components

Key foundation components for Kanpur Smart City considered for this RFP are as follows for implementation:

#	Component	Geographical Scope
1.	Network Backbone	As per requirement for field equipment's
2.	Command Control & Communication Centre	Located centrally at one location
3.	Data Centre and DR Site	▪ Smart and energy efficient Data Centre located centrally with Command Control & Communication Centre ▪ Cloud DR set-up
4.	ITMS	
5.	Variable Message Sign Board	
6.	Public Address System	
7.	Emergency Call Box (ECB) System	
8.	City Wi-Fi	
9.	Smart Parking	
10.	Environmental Monitoring System	
11.	Enterprise GIS	
12.	Web Portal & Mobile App	City portal and mobile app to disseminate information, infographics and service delivery through integration with stakeholder departments

2.1 Components & Services Scope Overview

The selected MSI shall ensure the successful implementation of the proposed ICCC solutions as well as provide capacity building support to city authorities as per the scope of services described below. Any functionality not expressly stated in this document but required to meet the needs of the KSCL to ensure successful operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible. MSI shall implement and deliver the systems and components which are described in this RFP. MSI's scope of work shall include but will not be limited to the following broad areas. Details of each of these broad areas have also been outlined in Annexures:

1. **Assessment, Scoping and Survey Study**: Conduct a detailed assessment, survey, gap analysis, scoping study and develop a comprehensive project plan, including:
   a) Assess existing ICT systems ,Network connectivity within the city and the greenfield site for the scope items mentioned in this Volume of the RFP
   b) Conduct site survey for finalization of detailed technical architecture, gap analysis, final Bill of Quantities and project implementation plan

c) Conduct site surveys to identify the need for site preparation activities
d) Obtain site clearance obligations & other relevant permissions with the support of KSCL

2. **Design, Supply, Configuration, Installation, Implementation, Testing and Commissioning of the following primary components:**

a) Integrated Command and Control Centre
b) Smart Data Centre within ICCC Building
c) Disaster Recovery Centre (Hosted on cloud data centre of any MEITY empanelled Cloud Service Provider)
d) Smart Parking Management System
e) City Surveillance
f) Intelligent Traffic Management System
  - Adaptive Traffic Control System (ATCS)
  - Automatic Number Plate Recognition (ANPR) System
  - Red Light Violation Detection (RLVD) System
  - Speed Violation Detection (SVD) System
  - Traffic Violation Cameras
  - Variable Message Sign boards
  - Public Address (PA)
  - Emergency Call Box (ECB) System

g) Environmental Monitoring Sensors
h) City Web Portal & Mobile App
i) Enterprise GIS Portal
j) Public Wi-Fi Hotspots

The detailed requirements of the above would be delineated within the subsequent sections.

3. **Integration with following listed existing and proposed system ICT systems within KSCL ICT landscape, not limited to:**

- Smart Lighting
- ICT Enabled Solid Waste Management
- Intelligent Transportation System
- E-Challan System
- Public Bike Sharing
- Smart Water Supply System
- Smart Education
- Smart Health Management System

4. **Data Centre:** Provisioning of Hardware, Network and Software Infrastructure, which includes design, supply, installation and commissioning of ICT Infrastructure at the Command Control and Communication Centre; Smart Data Centre. This scope consist of:

a) Site preparation services
b) IT Infrastructure including server, storage, other required hardware, application portfolio, licenses
c) Command Centre infrastructure including operator Video Walls, workstations, IP phones, joystick controller etc.
d) Establishment of LAN and WAN connectivity at command centre and DC limited to scope of infrastructure procured for the project

e) Application integration services with the above identified applications

5. **Provisioning of City wide Network backbone within the city and the greenfield site**
   a) Assessment of ISP service provider available in city
   b) Connectivity between field device and DC and ICCC
   c) Connectivity between DC & proposed DR
   d) Internet Connectivity at DC
   e) Network shall be sized with sufficient capacity to support the redundancy and future traffic growth in order to complete traffic rerouting on the network in event of failure without affecting overall network performance.

6. **Capacity Building for KSCL and any other department which includes preparation of operational manuals, training documents and capacity building support, including:**
   a) Training of city authorities, operators and other stakeholders on operationalization of the system
   b) Support during execution of acceptance testing
   c) Preparation and implementation of the information security policy, including policies on backup and redundancy plan
   d) Preparation of revised KPIs for performance monitoring of various urban utilities monitored through the system envisaged to be implemented
   e) Developing standard operating procedures for operations management and other services to be rendered by ICCC
   f) Preparation of system documents, user manuals, performance manuals, Operation manual etc.

7. **Operations and Maintenance**
   MSI shall also be responsible for the maintenance and management of entire systems, solutions, application deployed as part of this RFP for a period of 5 year from the Go-Live date of implemented solutions KSCL in an efficient and effective manner.

2.2 Component Architecture

Indicative architecture of the components envisaged under the ““Integrated Command Control and Communication Centre” is as given below. 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 project and its intended use. MSI shall carry out the detail requirement analysis and finalize technical architecture in consultation with authority and its consultants. The architecture layers of the complete network of smart elements is as follows.

a) Sensor or Field instrument 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 intelligent traffic signals, cameras, enforcement sensors, emergency call boxes, etc. Kanpur city is expected to have environmental IoT sensors installed at multiple locations across the city, to measure & report ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity for decision makers to take preventive, pro-active and execute responses in case of emergency/natural calamity.

b) Data Collection and Transmitting Layer

Controller processes data, that is input from the sensor applies the logic of control and causes an output action to be generated. This signal may be sent directly to the controlled device or to other logical control functions and ultimately to the controlled device.

The controllers function is to compare its input (from the sensor) with a set of instructions such as set point, throttling range and action, then produce an appropriate output signal. It usually consists of a control response along with other logical decisions that are unique to the specific control application. After taking the logical decision of the information it will hand over the information to the next layer (Network Layer) which will subsequently available at the ICCC.

c) Network/Communication 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 wherever applicable. The network layer will be scalable such that additional sensors, actuators, display devices can be seamlessly added and more Wi-Fi spots created in future.

d) Data Centre Layer

The data Centre layer will house centralized computing power required to store, process and analyze 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.

e) 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 MSI 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, authorization, 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 GoI for various eGovernance applications.
- End device security, including physical security of all end devices such as display boards, emergency boxes, 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

f) 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 at KSCL. 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 system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within KSCL , etc.) and non-government agencies.

g) Service delivery and Publishing Layer

The output field devices 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 digital messaging boards, environmental data displays, etc. The command Centre publishes the information which will enable citizens and administrators alike to get a holistic view of city conditions. The implementation vendor will have to develop a command Centre at a site location determined by KSCL and web/ mobile based viewing tools for understanding the ambient city conditions.

3 Survey, Deign Consideration for finalization of detailed technical architecture and project plan

After signing of contract, the Systems Integrator needs to deploy local team (based out of KSCL) proposed for the project and ensure that a Project Inception Report is submitted to KSCL which should cover following aspects:

1. Names of the Project Team members, their roles & responsibilities and deliverables
2. Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project)
3. Responsibility assignment matrix for all stakeholders
4. Risks that MSI anticipates and the plans they have towards their mitigation
5. Detailed project plan specifying dependencies between various project activities / sub-activities and their timelines
6. Installation locations for field devices geo mapped to visually identify the geographical area

MSI shall conduct a comprehensive As-Is study of the existing system and infrastructure. The report shall also include the expected measurable improvements against each KPI in ‘As-Is’ study after implementation of smart solutions under this project. The benchmarking data should also be developed to track current situation and desired state.

MSI shall study the existing business processes, functionalities, existing systems and applications including MIS reporting requirements.

MSI will be responsible to propose transition strategy for dismantling of existing signals, and setting up of new smart signals and field components. The proposed strategy should clearly provide approach and plan for implementing the new signals and field components while ensuring minimum disturbance to the road traffic and shall use appropriate static signage designating the work in progress status.

Additionally, MSI should provide a detailed To-Be designs specifying the followings:

1. High Level Design (including but not limited to) Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams and other data modelling documents and Physical infrastructure design for devices on the field
2. Application component design including component deployment views, control flows, etc.
3. Low Level Design (including but not limited to) Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid-down by Government of India.
4. Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on map) with GEO coordinates.
5. Height and foundation of Cameras, Traffic Signals and Poles for Pedestrian signals, Height and foundation of Poles, cantilevers, gantry and other mounting structures for other field devices
6. Location of Junction Boxes, Wi-Fi Access Points
9. Electrical power provisioning

MSI shall also identify the customizations/ workaround that would be required for successful implementation and operation of the project. The report should take into consideration following guiding principles:

- **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.

- **Use Of Open Standard for evolving Technology :T**he 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.

- **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.

- **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. SI 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 controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. 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. Bidder'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).

  Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI shall be required to repair / replace any equipment if stolen / damaged/faulty. 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 Centre (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 talk only to the authorized 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 ID, Device ID etc.
- 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.

- **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 data centre infrastructure shall be capable of serving at least 1000 concurrent users. 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.

- **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.
  - Network, DC, DR should be available 99.95 % time.
  - Comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time)
  - Provide analytic tools build into the system that shall support automatic detection of anomalies and their quick mitigation.

- **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

- **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 SI 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:

  (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 standards and as per standards mentioned at Annexure –V.

All the personnel working on the Project and having access to the Servers / Data Center should be on direct payroll of the SI/OEM/Consortium partner. The SI would not be allowed to sub-contract work, except for following:

- Passive networking & civil work during implementation and O&M period,
- Viewing manpower at Command/ viewing centres & Mobile Vans during post-implementation
- FMS staff for non- IT support during post-implementation

However, even if the work is sub-contracted, the sole responsibility of the work shall lie with the MSI. The MSI shall be held responsible for any delay/error/non-compliance/penalties etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to city and approved by the Authority before resource mobilisation.

- **Convergence -** KSCL 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, KSCL has envisaged to create a state of the art infrastructure and services for the citizens of KSCL, 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 KSCL. The procedure for utilization of the infrastructure will be mutually agreed between the KSCL and MSI

Sub-contracting / Outsourcing shall be allowed only for the work which is mentioned in the relevant clauses of Volume I of this RFP with prior written approval of KSCL. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with MSI. MSI shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor. The details of the sub-contracting agreements (if any) between both the parties would be required to be submitted to KSCL.

- **GIS Integration-** MSI shall undertake detail assessment for integration of the Smart Governance, Surveillance System and all other components with the Geographical Information System (GIS). MSI is required to carry out the seamless integration to ensure ease of use of GIS in the Dashboards in Command Control Centers. If this requires field survey, it needs to be done by MSI. If such a data is already available with city, it shall facilitate to provide the same. MSI is to check the availability of such data and it's suitability for the project.SI is required to update GIS maps from time to time.

- **SMS Gateway Integration-** MSI shall carry out SMS Integration with the Smart City System and develop necessary applications to send mass SMS to groups/individuals. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.

- **Application Architecture**

  I. 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 standards and as per standards mentioned at Annexure –V.

  II. 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.

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

I. The Modules specified will be developed afresh based on approved requirement.

II. Apart from this, if some services are already developed/under development phase by the specific department, such services will be integrated with the Smart City System. These service will be processed through department specific Application in backend.

III. The user of citizen services should be given a choice to interact with the system in local language in addition to English. The application should provision for uniform user experience across the multi lingual functionality covering following aspects:
   - Front end web portal in English and local language
   - E-forms (Labels & Data entry in local languages). Data entry should be provided preferably using the Enhanced Inscript standard (based on Unicode version 6.0 or later) keyboard layout with option for floating keyboard.
   - Storage of entered data in local language using UNICODE (version 6.0 or later) encoding standard.
   - Retrieval & display in local language across all user interfaces, forms and reports with all browsers compliant with Unicode version 6.0 and above.
   - Facility for bilingual printing (English and the local language)

IV. Application should have a generic workflow engine for citizen centric services. This generic workflow engine will allow easy creation of workflow for new services. At the minimum, the workflow engine should have the following features:
   - Feature to use the master data for the auto-populating the forms and dropdowns
   - Creation of application form, by “drag & drop” feature using meta data standards
      i. Defining the workflow for the approval of the form
      ii. First in First out
      iii. Defining a citizen charter/ delivery of service in a time bound manner
   - Creation of the “output” of the service, i.e. Certificate, Order etc.
   - Automatic reports
      iv. of compliance to citizen charter on delivery of services
      v. delay reports

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 standards and /or as per standards mentioned at Annexure –XI.

V. The application should have a module for management of digital signature including issuance, renewal and suspension of digital signatures based on the administrative decisions taken by the State.

- SI shall ensure using Digital signatures/eAuthentication(Aadhar Based) to authenticate approvals of service requests etc.

VI. e-Transaction & SLA Monitoring Tools

A. The SI should be able to measure and monitor the performance of the deployed infrastructure and all SLAs set out in this RFP. More importantly, it should be possible to monitor in REALTIME, the number of citizens touched through e-Services each day, month and year, through appropriate tools and MIS reports.

B. The Infrastructure management and Monitoring System shall be used by SI to monitor the infrastructure (Both IT and Non-IT) hosted at the Data center and DR site..

C. for monitoring of uptime and performance of IT and non IT infrastructure deployed , the SI shall have to provision for monitoring and measurement tools, licenses, etc. required for this purpose.

VII. The Smart City Application should have roadmap to integrate with key initiatives of State namely Portal Services, Citizen Contact Centre, Certifying Authority etc.

VIII. Complete mobile enablement of the Smart City System

Other expectations from SI

1. MSI shall engage early in active consultations with the Authority , City Police and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.
2. Study the existing fiber duct (if any) layout in the city and existing network to understand the existing technology adopted in each of the following areas (not limited to):

i- City WiFi

ii- Surveillance Infrastructure – CCTV Cameras, Data communication, monitoring, control room and Infrastructure

iii- Other Smart City initiatives envisaged

3. MSI shall assess existing infrastructure’s current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible
4. MSI shall judiciously evaluate the resources and time planned for undertaking the current state assessment, given the overall timelines and milestones of the project.
5. MSI shall be responsible for supply of all the Products/equipment such as optical fiber cable, Network, Hardware, Software, Devices, etc. as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.
6. MSI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fiber Patch Cords, Racks etc. Civil work required for the site shall be undertaken by the MSI.
7. Validate / Assess the re-use of the existing infrastructure if any with Authority site

8. Supply, Installation, and Commissioning of entire solution at all the locations.
9. MSI shall provide the bandwidth required for operationalizing each smart city initiative till the time Authority's own fiber is laid by the MSI as part of the scope of work of this RFP. The bandwidth requirement shall be analysed and procured by the MSI at its own cost / risk.
10. MSI shall Install and commission connectivity across all designated locations.
11. MSI shall establish high availability, reliability and redundancy of the network elements to meet the Service Level requirements.
12. MSI shall be responsible for planning and design of the access network architecture (access controllers, backhaul connectivity, routers, switches, etc.) to meet the technical, capacity and service requirements for all smart city initiatives.
13. MSI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by Authority.
14. MSI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months from the date of bidding
15. MSI shall ensure that the end of support is not reached during the concurrency of the contract and 5 years thereafter.
16. MSI shall ensure compliance to all mandatory government regulations as amended from time to time.
17. The MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords (fiber), cables, software, licenses, tools, etc. are provided according to the requirements of the solution.
18. Authority shall not be responsible if the MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the RFP. The MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to Authority.
19. All the software licenses that the SI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and Authority shall have the flexibility to use the software licenses for other requirements if required.
20. The SI shall ensure there is a 24x7 comprehensive onsite support for duration of the contract for respective components to meet SLA requirement. The SI shall ensure that all the OEMs have an understanding of the service levels required by Authority. SI is required to provide the necessary MAF (Manufacturer Authorization Form) as per the format provided in the RFP in support of OEMs active support in the project.
21. Considering the criticality of the infrastructure, SI is expected to design the solution considering the RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.
22. SI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.

23. SI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.
24. SI is expected to provide following services, including but not limited to:

    i. Provisioning hardware and network components of the solution, in line with the proposed authority's requirements
    ii. Size and propose for network devices (like Router, switches, security equipment including firewalls, IPS / IDS, routers, etc. as per the location requirements with the required components/modules, considering redundancy and load balancing in line with RFP.
    iii. Size and provision the WAN bandwidth requirements across all locations considering the application performance, data transfer, DR and other requirements for smart city initiatives.
    iv. Size and provision the internet connectivity for Service Provider network and Network Backbone.
    v. Size and provision for bandwidth as a service for operations of City WiFi, City Kiosk, CCTV surveillance till operationalization of network backbone
    vi. Liaise with service providers for commissioning and maintenance of the links.
    vii. Furnish a schedule of delivery of all IT/Non-IT Infrastructure items
    viii. All equipment proposed as part of this RFP shall be rack mountable.
    ix. Authority may at its sole discretion evaluate the hardware sizing document proposed by the SI. The. SI needs to provide necessary explanation for sizing to the Authority
    x. Complete hardware sizing for the complete scope with provision for upgrade
    xi. Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
    xii. The SI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
    xiii. The SI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/management through SNMP from the date of installation by a Network Monitoring System.

Note:

1) The 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; and
2) MSI has to deploy the all the solutions with disable friendly features with in it to enable the more usage and help all type of users.

3.1 Commencement of Works

Site Clearance obligations & other relevant permissions –

Prior to starting the site clearance, MSI shall carry out survey of field locations as specified in RFP, for buildings, structures, fences, trees, existing installations, etc. The KSCL shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the KSCL before executing the plan

3.2 Existing Traffic Signal system

The infrastructure of existing traffic signal systems including the aspects, controllers etc. will be dismantled and replaced with the new systems where required, which are proposed and required under the scope of the ITMS. The dismantled infrastructure shall be delivered at the KSCL designated location without damage at no extra cost.

3.3 Road signs

All existing road signs which are likely to be effected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with KSCL guidelines. Road signs, street name plate, etc. damaged during their operation by MSI shall be repaired or replaced by MSI at no additional cost.

3.4 Electrical works and power supply

MSI shall directly interact with electricity board for provision of mains power supply at all desired locations for ITMS field solution. MSI shall be responsible to submit the electricity bill including connection charge, meter charge, recurring charges etc. to the electricity board directly. MSI shall have to submit the challan of bill submission to KSCL. KSCL will reimburse the amount submitted to MSI after verification in next billing cycle.

3.5 Lightning-proof measures

MSI shall comply with lightning-protection and anti –interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. MSI shall describe the planned lightning-protection and anti –interference measures in the As-Is report. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function & should be capable to bear certain mechanical external force. Signal separation of low and high frequency; equipment's protective field shall be connected with its own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling. The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.Type 1 device shall be installed between zone 0B and zone 1. Type 2 devices shall be installed before the equipment in zone 2 and 3.

3.6 Earthing System

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. The entire applicable IT infrastructure i.e. signal junction or command centre shall have adequate earthing. Further, earthling should be done as per Local state national standard in relevance with IS standard.

1. Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. KSCL shall provide the necessary space required to prepare the earthing pits.
2. All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
3. 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.
4. The earth connections shall be properly made.
5. 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 needs to be in place for this copper mesh.
6. Provide separate Earthing pits for Servers, & UPS as per the standards.
7. The metallic housing of electronic equipment/junction box/panel shall be connected to the earthing system
8. The active electronic parts of an electronic equipment system shall be connected to the earthing system

3.7 Junction Box, Poles and Cantilever

1. MSI shall provide the Junction Boxes, posts and cantilever to mount the field sensors like the cameras, traffic sensors, traffic light aspects, active network components, controller and power backup (UPS/Alternate energy sources) at all field locations, as per the specifications given in the RFP.
2. Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions, and MSI should design the Junction box for 1.5 times the actual size MSI requires for utilization under the ITMS project.
3. Additional 50% space in the Junction Box shall be utilized by KSCL to accommodate any future requirements under other projects
4. Junction Box for UPS with Battery bank needs to be considered separately. Bidder may propose solar based solutions to power the equipment. In this case, raw power can be used as backup supply whenever solar power is not able to meet the requirement.
5. It should be noted that MSI would have designed the Junction box keeping in mind the scalability requirements of ITMS project, and the additional 50% volume needs to considered over and above such requirement
6. The junction box should be designed in a way that, separate compartment will be available for separate system (i.e. ITMS Controller, Mini server, Active component, etc.). Each compartment shall have lock & key facility. There should be provision made to integrate the systems if required.

3.8 Cabling Infrastructure

1. MSI shall provide standardized cabling for all devices and subsystems.
2. MSI shall ensure the installation of all necessary cables and connectors between the field sensors /devices assembly, outstation junction box, for pole mounted field sensors/devices the cables shall be routed down the inside of the pole and

through underground duct to the outstation cabinet.

3. All cables shall be clearly labeled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards.
4. Cabling must be carried out per relevant BIS standards. All cabling shall be documented in a cable plan by MSI.

3.9 Integrated Command & Control Centre (ICCC)

The vision of the Command and Control (ICCC) is to have an integrated view of all the smart initiatives undertaken by KSCL with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. ICCC involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. ICCC shall be a fully integrated solution that provides seamless traffic management, incident – response management, collaboration and geo-spatial display. This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices. Following are the integration capabilities from this platform. 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 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.

ICCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials. Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion. ICCC should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Parking, BRT, Sewerage/ Drainage system, Disaster Mgmt. System etc.

MSI has to integrate all smart components of the project at Command Control and Communication Centre with an integrated operations and dashboard application that will integrate various Smart City components implemented in this project and in future.

As part of this RFP, MSI shall ensure that redundancy and fault tolerance is considered at the ICCC components level in the actual deployment.

High Availability / Up Time Targets for ICCC operations are identified as follows:

- Availability Target (24Hr operation): 99.582%
- Maximum Downtime Tolerated per Day: 6 minutes
- Maximum Downtime Tolerated per Week: 42 minutes

Integrated city operation platform should be able to carter to following requirements;

1. Urban Services and Data APIs:

a. **Live data** and **visual feed** from diverse sensors should be connected to the platform

b. **Normalized APIs:** for listed domain (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality

   i. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality

c. **Cross APIs Integration:** Enabling contextual information (API-API Bi-directional) and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)

2. Platform functionality:

a. **API management and gateway:** Provides secure API lifecycle, monitoring mechanism for available APIs

b. **User and subscription management:** Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions

c. **Application management:** Provides role-based access view to applications

d. **Enabling analytics:** Time shifted and real-time data available for big data and analytics

e. **Domain and/or Insight reports**

   i. Parking occupancy, energy reports, AQI report (environmental pollution)

3.10 Data Centre and Disaster Recovery Centre

- KSCL shall provide the location to house the compute and storage infrastructure, at the Data Centre facility being built at the Command and Control Centre. The KSCL has identified the location for ICCC and DC to be within the premise of Municipal Corporation.
- The DR for the data centre shall be on cloud on empanelled service providers by MeiTY
- Various ICT equipment to be provisioned and maintained by MSI at the Data Centre is given below.
- Only the minimum specifications for the active and passive ICT and Non-ICT components are specified.
- MSI may propose Data Centre Virtualisation solution for price discovery
- MSI shall peruse the same provide the BOM / BOQ required to the meet the performance requirements as per the proposed business needs. MSI may also suggest additional components as per the solution requirements.
- The information between the Smart DC and the DR cloud shall be synchronised over the network such that that the smart city solutions are high available on the network
- Operational and Uptime Requirements for Data Centre

I. Minimum Tier Rating for Data Centre: **Tier 3**

   a. Availability Target (24Hr operation): 99.741%
   b. Maximum Downtime Tolerated per Day: 4 minutes
   c. Maximum Downtime Tolerated per Week: 27 minutes
   d. Maximum Downtime Tolerated per Month: 1 hours 54 minutes
   e. Maximum Downtime Tolerated per Quarter: 5 hours 42 minutes

f. Maximum Downtime Tolerated per Year: 22 hours 43 minutes

II. Operational Compliance Requirements for MSI operations:
a. PCI-DSS
b. ISO 27001
c. ISO 20000
d. Cyber Security Framework for Smart City (MoUHA)

Note: Operational Compliance applicable for Data Centre, ICCC and NOCs

4 Other Expectation and Consideration from MSI

4.1 Inception Phase

MSI will be responsible for preparation of detailed project plan. The plan shall address at the minimum the following:

i. Define an organized set of activities for the project and identify the interdependence between them.

ii. Resource planning and loading for each phase/activity. This must also indicate where each resource would be based during that phase, i.e. onsite at the KSCL office or off site at MSI premises.

iii. Establish and measure resource assignments and responsibilities

iv. Highlight the milestones and associated risks

v. Communicate the project plan to stakeholders with meaningful reports.

vi. Measure project deadlines and performance objectives.

vii. Project Progress Reporting. During the implementation of the project, MSI should present weekly reports. This report will be presented in the steering committee meeting to KSCL. The report should contain at the minimum the under mentioned:

a. Results accomplished during the period (weekly)

b. Cumulative deviations from the schedule date as specified in the finalized Project Plan

c. Corrective actions to be taken to return to planned schedule of progress

d. Plan for the next week

e. e. Proposed revision to planned schedule provided such revision is necessitated by reasons beyond the control of MSI

f. Support needed

g. Highlights/lowlights

h. Issues/Concerns

i. Risks/Show stoppers along with mitigation

viii. Identify the activities that require the participation of client personnel (including KSCL, the Program Management Unit etc.) and communicate their time requirements and schedule early enough to ensure their full participation at the required time.

4.2 Requirement Phase

MSI must perform the detailed assessment of the business requirements and IT Solution requirements as mentioned in this RFP. Based on the understanding and its own individual assessment, MSI shall develop & finalize the System Requirement Specifications (SRS) in consultation with KSCL and its representatives. While doing so, MSI at least is expected to do following:

a. MSI shall conduct a detailed survey and prepare a gap analysis report, detailed survey report of the physical and field infrastructure requirements. MSI shall duly assist the department in preparing an action plan to address the gaps.

b. MSI shall study and revalidate the requirements given in the RFP with KSCL and submit as an exhaustive FRS document. MSI shall develop the FRS and SRS documents.

c. MSI shall develop and follow standardized template for requirements capturing and system documentation.

d. MSI must maintain traceability matrix from SRS stage for the entire implementation.

e. MSI must get the sign off from user groups formed by KSCL.

f. For all the discussion with KSCL team, MSI shall be required to be present at KSCL office with the requisite team members.

g. Prior to starting the site clearance, MSI shall carry out survey of field locations as specified in Annexure IX, for buildings, structures, fences, trees, existing installations, etc.

h. The infrastructure of existing traffic signal and other street ICT infrastructure may need to be dismantled and replaced with the new systems which are proposed and required under the scope of the project. The infrastructure such as poles, cantilevers, cabling, aspects etc. should be reused to derive economies for the project with prior approval of KSCL. The dismantled infrastructure shall be delivered at the KSCL designated location without damage at no extra cost.

i. All existing road signs which are likely to be effected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with KSCL guidelines. Road signs, street name plate, etc. damaged by MSI during their operation shall be repaired or replaced by MSI at no additional cost.

j. MSI shall directly interact with electricity boards for provision of mains power supply at all desired locations for field solution. KSCL shall facilitate the same. The recurring electricity charges will be borne by KSCL as per actual consumption.

4.3 Design Phase

MSI shall build the solution as per the Design Considerations detailed in Annexure – III. The solution proposed by MSI should comply with the design considerations requirements as mentioned therein.

4.4 Development Phase

MSI shall carefully consider the scope of work and provide a solution that best meets the project's requirements. Considering the scope set in this RFP, MSI shall carefully consider the solutions it proposes and explicitly mention the same in the technical proposal. The implementation of the application software will follow the procedure mentioned below:

a. Software Products (Configuration and Customization): In case MSI proposes software products the following need to be adhered:

   i. MSI will be responsible for supplying the application and licenses of related software products and installing the same so as to meet project requirements.

ii. MSI shall have provision for procurement of licenses in a staggered manner as per the actual requirement of the project.

ii. MSI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. MSI shall report any exceptions to license terms and conditions at the right time to KSCL. However, the responsibility of license compliance solely lies with MSI. Any financial penalty imposed on KSCL during the contract period due to license non-compliance shall be borne by MSI.

iii. As per requirement of complex solution implementation MSI has to put requirement that OEM own resource & MSI best technical resources are deployed in this project.

iv. The OEM should provide the specific Designing (OEM Low Level Design, Core Implementation) support expertise to make sure that their supplied technology & products work as per the design objectives.

v. OEM to design and implement the complete security policy and workflow as per industry best practice in consultation with Customer to meet their Business requirements

vi. MSI should provide the overall program management and OEM to ensure that the solution which may include multiple technologies from various OEM, to work together seamlessly as per the design goals. The seamless integration with all devices would be SI responsibility for the respective products offered.

vii. For Core, Due to large no of devices only 20% of the equipment to be deployed by OEM own the MSI as per OEM provided design shall deploy technical resources and rest including Access/Remote.

iv. MSI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, MSI shall supply:

a) Software & licenses.

b) Supply tools, accessories, documentation and provide a list of the same. Tools and accessories shall be part of the solution.

c) System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following. Documentation to be maintained, updated and submitted to KSCL regularly :

- Functional Requirement Specification (FRS)
- High level design of whole system
- Low Level design for whole system / Module design level
- System Requirements Specifications (SyRS)
- Any other explanatory notes about system
- Traceability matrix
- RACI Matrix
- Technical and product related manuals
- Installation guides
- User manuals

- System administrator manuals
- Toolkit guides and troubleshooting guides
- Other documents as prescribed by KSCL
- Quality assurance procedures
- Change management histories
- Version control data
- SOPs, procedures, policies, processes, etc. developed for KSCL
- Programs :
    - Entire source codes as applicable
    - All programs must have explanatory notes for understanding
    - Version control mechanism
    - All old versions to be maintained
    - Test Environment :
    - Detailed Test methodology document
    - Module level testing
    - Overall System Testing
    - Acceptance test cases

(These documents need to be updated after each phase of project and to be maintained updated during entire project duration. The entire documentation will be the property of KSCL.)

4.5 Integration Phase

The Command and control Centre should be integrated with feeds of all tracks/component through OPC UA (OLE Platform Communication) deployed under this KSCL Project. MSI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution as a whole. The testing should be comprehensive and should be done at each stage of development and implementation.to enable city for batter decision management and planning

4.6 Pilot Deployment

- MSI shall conduct Pilot deployment and testing for meeting KSCL’s business requirements before rolling out the complete system. The pilot will be run for four weeks to study any issues arising out of the implementation. MSI shall also review health, usage and performance of the system till it is stabilized during pilot deployment. Based on KSCL’s feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Pilot implementation.
- Pilot shall be demonstrated to the KSCL’s representatives. If for any reason the pilot is found to be incomplete, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the Pilot may lead to termination of the contract with no liability to Client.

4.7 Go-Live Preparedness and Go-Live

- MSI shall prepare and agree with KSCL, the detailed plan for Go-Live (in-line with KSCL's implementation plan as mentioned in RFP).
- MSI shall define and agree with KSCL, the criteria for Go-Live.
- MSI shall ensure that all the data migration is done from existing systems.
- MSI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.
- MSI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and MSI needs to take approval from KSCL team on the same.
- Go-live of the application shall be done as per the finalized and agreed upon Go-Live plan.

4.8 Handholding and Training

In order to strengthen the staff, structured capacity building programmes shall be undertaken for identified resources of KSCL, Corporation, UD&HD and stakeholder departments. It is important to understand the 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. The actual number of trainees will be provided at design stage.

a) MSI shall prepare and submit detailed Training Plan and Training Manuals to KSCL for review and approval.

b) 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.

c) MSI shall also be responsible for full capacity building. Training and capacity building shall be provided for all individual modules along with their respective integrations.

d) MSI shall be responsible for necessary demonstration environment setup including setup of cameras, Wi-Fi, sensors and application 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 CCC, DC, field locations etc. End user training shall be conducted at a centralized location or any other location as identified by KSCL with inputs from the MSI.

e) 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.

f) MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the ICCC system.

g) MSI shall prepare the solution specific training manuals and submit the same to KSCL for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in Hindi & English language.

h) MSI shall provide training to selected officers of the purchaser covering functional, technical aspects, usage and implementation of the products and solutions.

i) 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.

j) An annual training calendar shall be clearly chalked out and shared with the KSCL along with complete details of content of training, target audience for each year etc.

k) 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.

l) MSI shall ensure that training is a continuous process for the users. Basic intermediate and advanced application usage modules shall be identified by the MSI.

m) 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.

n) Time Schedule and detailed program shall be prepared in consultation with KSCL and respective authorized entity. 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.

o) MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.

p) The master trainers shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the KSCL feels that on-field sessions are required, the same shall be conducted by the MSI.

q) If any trainer is considered unsuitable by KSCL, either before or during the training, MSI shall provide a suitable replacement without disrupting the training plan.

r) Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.

s) KSCL shall be responsible for identifying and nominating users for the training. However, SI shall be responsible for facilitating and coordinating this entire process.

t) MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive feedback mechanism. MSI shall be responsible for making the feedback available for the KSCL/authorized entity to review and track the progress, In case, after feedback, more than 40% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the SI shall re-conduct the same training at no extra cost.

Types of Trainings: Following training needs is identified for all the project stakeholders:

I. Functional Training

- ✓ Basic IT skills
- ✓ Web portal, Mobile App, Enterprise GIS, ITMS, Smart Parking, Wi-Fi, environmental sensors, Data Analytics, ANPR, smart solutions etc.
- ✓ Software Applications (Command Control and Communication Centre)
- ✓ Networking, Hardware Installation
- ✓ Centralized Helpdesk
- ✓ Feed monitoring

II. Administrative Training

- ✓ System Administration Helpdesk, BMS Administration etc.
- ✓ Master trainer assistance and handling helpdesk requests etc.

III. Senior Management Training

- ✓ Usage of all the proposed systems for monitoring, tracking and reporting,
- ✓ MIS reports, accessing various exception reports

IV. Post-Implementation Training

- ✓ Refresher Trainings for senior officials
- ✓ Functional/Operational training and IT basics for new operators
- ✓ Refresher courses on System Administration
- ✓ Change Management programs

4.9 Operations and Maintenance

MSI will operate and maintain all the components of the ICCC System for a period of five (5) years after Go-Live date. During O&M phase, MSI shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to KSCL. After Go-Live, if any system/sub-system/appliance that is deployed during the O&M phase must be added in the System only after proper induction procedures are followed including hardening and security testing. MSI needs to implement suitable Performance Improvement Process (PIP) in the project.

PIP program applies to all the processes of ICCC project. MSI need to submit its detailed approach for PIP in its technical proposal. Every process and procedure implemented in this project must be reviewed and updated by MSI at least on annual basis from the Go-Live Date. All the manpower engaged for O&M support of the project should be citizens of India. MSI will ensure that at no time shall any data of ICCC System be ported outside the geographical limits of the country. Some broad details of O&M activities are mentioned at later sections.

4.9.1 Applications Support and Maintenance

Application support includes, but not limited to, production monitoring, troubleshooting and addressing the functionality, availability and performance issues, implementing the system change requests etc. The MSI shall keep the application software in good working order; perform changes and upgrades to applications as requested by the KSCL team. All tickets related to any issue/complaint/observation about the system shall be maintained in an ITIL compliant comprehensive ticketing solution. Key activities to be performed by MSI in the application support phase are as follows:

a. Compliance to SLA

MSI shall ensure compliance to SLAs as indicated in this RFP and any upgrades/major changes to the software shall be accordingly planned by MSI ensuring the SLA requirements are met at no additional cost to the KSCL.

b. Annual Technology Support

MSI shall be responsible for arranging for annual technology support for the OEM products to RSSCCL provided by respective OEMs during the entire O&M phase.

c. Application Software Maintenance

i. MSI shall provide unlimited support through onsite team/telephone/Fax/E-mail/Video Conferencing/installation visit as required

ii. MSI shall address all the errors/bugs/gaps in the functionality in the solution implemented by the MSI (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the O&M phase.

iii. All patches and upgrades from OEMs shall be implemented by the MSI ensuring customization done in the solution as per the KSCL's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the MSI. Any version upgrade of the software / tool / appliance by MSI to be done after taking prior approval of KSCL and after submitting impact assessment of such upgrade.

iv. Any changes/upgrades to the software performed during the support phase shall subject to the comprehensive and integrated testing by the MSI to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system. Release management for application software will also require KSCL's approval. A detailed process in this regard will be finalized by MSI in consultation with KSCL.

v. Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the MSI and periodically submitted to the

KSCL.

vi. MSI, at least on a monthly basis, will inform KSCL about any new updates/upgrades available for all software components of the solution along with a detailed action report.

vii. In case of critical security patches/alerts, the MSI shall inform about the same immediately along with his recommendations. The report shall contain MSI's recommendations on update/upgrade, benefits, impact analysis etc. The MSI shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, MSI will carry it out free of cost by following defined process.

d. Problem identification and Resolution

i. Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. MSI shall identify and resolve all the application problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).

ii. Monthly report on problem identified and resolved would be submitted to KSCL along with the recommended resolution.

e. Change and Version Control

All planned or emergency changes to any component of the system shall be through the approved Change Management process. The MSI needs to follow all such processes (based on industry ITSM framework). For any change, MSI shall ensure:

i. Detailed impact analysis

ii. Change plan with Roll back plans

iii. Appropriate communication on change required has taken place

iv. Proper approvals have been received

v. Schedules have been adjusted to minimize impact on the production environment

vi. All associated documentations are updated post stabilization of the change

vii. Version control maintained for software changes

The MSI shall define the Software Change Management and Version control process. For any changes to the solution, MSI has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. MSI shall ensure that software and hardware version control is done for entire duration of MSI's contract

f. Maintain configuration information

MSI shall maintain version control and configuration information for application software and any system documentation.

g. Training

MSI shall provide training to KSCL personnel whenever there is any change in the functionality. Training plan has to be mutually decided with KSCL.

h. Maintain System documentation

MSI shall maintain at least the following minimum documents with respect to the ICCC System:

i. High level design of whole system

ii. Low Level design for whole system / Module design level

iii. System requirements Specifications (SRS)

iv. Any other explanatory notes about system

v. Traceability matrix

vi. Compilation environment

MSI shall also ensure updation of documentation of software system ensuring that:

i. Source code is documented

ii. Functional specifications are documented

iii. Application documentation is updated to reflect on-going maintenance and

iv. enhancements including FRS and SRS, in accordance with the defined standards

v. User manuals and training manuals are updated to reflect on-going

vi. changes/enhancements

vii. Standard practices are adopted and followed in respect of version control and management.

i. All the project documents need to follow version control mechanism. MSI will be required to keep all project documentation updated and should ensure in case of any change, the project documents are updated and submitted to KSCL by the end of next quarter.

j. For application support MSI shall keep dedicated software support team to be based at MSI location that will single point of contact for resolution of all application related issues. This team will receive all the application related tickets/incidents and will resolve them. In its technical proposal MSI need to provide the proposed team structure of application support including number of team members proposed to be deployed along with roles and skills of each such member. Application support team shall be employees of MSI

k. 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.

l. Any additional changes required would follow the Change Control Procedure. KSCL may engage an independent agency to validate the estimates submitted by the MSI. The inputs of such an agency would be taken as the final estimate for efforts required. MSI to propose the cost of such changes in terms of man month rate basis and in terms of Function point/Work Breakdown Structure (WBS) basis in the proposal.

4.9.2 ICT Infrastructure Support and Maintenance

ICT infrastructure includes servers, storages, back up, networking, load balancers, security equipment, operating systems, database, enterprise management system, help desk system and other related ICT infra required for running and operating the envisaged system. MSI shall define, develop, implement and adhere to IT Service Management (ITSM) processes aligned to ITIL framework for all the IT Services defined and managed as part of this project.

4.9.3 Warranty support

a. MSI shall provide comprehensive and on-site warranty for 5 years from the date of Go-Live for the infrastructure deployed on the project. MSI need to have OEM support for these components and documentation in this regard need to be submitted to KSCL on annual basis.

b. MSI shall provide the comprehensive & onsite manufacturer's warranty in respect of proper design, quality and workmanship of all hardware, equipment, accessories etc. covered by the RFP. MSI must warrant all hardware, equipment, accessories, spare parts, software etc. procured and implemented as per this RFP against any manufacturing defects during the warranty period.

c. MSI shall provide the performance warranty in respect of performance of the installed hardware and software to meet the performance requirements and service levels in the RFP.

d. MSI is responsible for sizing and procuring the necessary hardware and software licenses as per the performance requirements provided in the RFP. During the warranty period MSI shall replace or augment or procure higher-level new equipment or additional licenses/hardware at no additional cost to the RSCL in case the procured hardware or software is not enough or is undersized to meet the service levels and the project requirements.

e. During the warranty period MSI shall maintain the systems and repair/replace at the installed site, at no charge to KSCL, all defective components that are brought to the MSI's notice.

f. The MSI shall carry out Preventive Maintenance (PM) of all hardware and testing for virus, if any, and should maintain proper records at each site for such PM. The PM should be carried out at least once in six months as per checklist and for components agreed with KSCL.

g. The MSI shall carry out Corrective Maintenance for maintenance/troubleshooting of supplied hardware/ software and support infrastructure problem including network (active/passive) equipment, security and rectification of the same. The MSI shall also maintain complete documentation of problems, isolation, cause and rectification procedures for building knowledge base for the known problems in centralized repository, accessible to KSCL team as well.

h. MSI shall monitor warranties to check adherence to preventive and repair maintenance terms and conditions.

i. The MSI shall ensure that the warranty complies with the agreed technical standards, security requirements, operating procedures, and recovery procedures.

   i. MSI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met.

   ii. Any component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA).

   iii. The MSI shall introduce a comprehensive Assets Management process & appropriate tool to manage the entire lifecycle of every component of ICCC system.

4.9.4 Maintenance of ICT Infrastructure at the DC and ICCC

a. Management of DC and ICCC

MSI need to deploy requisite mix of L1, L2 and L3 resources (on 24X7 basis) for management of entire ICCC System including ICT infrastructure deployed at DC and ICCC. All resources deployed in the project should be employees of MSI and be Indian citizens. All the L1 and L2 resources proposed for the project need to be dedicated for the project. Any change in the team once deployed will require approval from KSCL. It is expected that resources have proven track record and reliability. Considering the criticality of the project, KSCL may ask for security verification (Police verification) of every resource deployed on the project and MSI need to comply the same before deployment of the resource at the project. At all times, the MSI need to maintain the details of resources deployed for the project to KSCL and keep the same updated. A detailed process in this regard will be finalised between KSCL and MSI. The MSI shall maintain an attendance register for the resources deployed Attendance details of the resources deployed also need to be shared with KSCL on monthly basis. KSCL reserves the right to interview resources deployed for Operations and maintenance and assess the suitability of the resource for the role. In case a resource is not found suitable, MSI will change the resource on request of KSCL. MSI shall comply with this.

The scope of work for infrastructure and maintenance includes the following:

i. DC operations to be in compliance with industry leading ITSM frameworks like ITIL, ISO

ii. 20000 & ISO 27001

iii. Ensure compliance to relevant SLA’s

iv. 24x7 monitoring & management of availability & security of the infrastructure and assets

v. Perform regular hardening, patch management, testing and installation of software updates issued by OEM/vendors from time to time after following agreed process

vi. Ensure overall security – ensure installation and management of every security component at every layer including physical security

vii. Prepare documentation/policies required for certifications included in the scope of work

viii. Preventive maintenance plan for every quarter

ix. Performance tuning of system as required

x. Design and maintain Policies and Standard Operating Procedures

xi. User access management

xii. Other activities as defined/to meet the project objectives

xiii. Updation of all Documentation.

During operations phase the MSI needs to submit proof of renewal of support for all IT infrastructure products and other system software’s for whom it is mandated to have OEM support.

This needs to be submitted on an annual basis and needs to be verified before release of 2nd quarter payment of each year.

b. System Maintenance and Management

i. MSI shall be responsible for tasks including but not limited to setting up servers, configuring and apportioning storage space, account management, performing periodic backup of data and automating reporting tasks, and executing hardware and software updates when necessary. It shall be noted that the activities performed by the MSI may also be reviewed by KSCL.

ii. MSI shall provision skilled and experienced manpower resources to administer and manage the entire system at the Data Center.

iii. On an ongoing basis, MSI shall be responsible for troubleshooting issues in the IT infrastructure solution to determine the areas where fixes are required and ensuring resolution of the same.

iv. MSI shall be responsible for identification, diagnosis and resolution of problem areas pertaining to the IT Infrastructure and maintaining the defined SLA levels.

v. MSI shall implement and maintain standard operating procedures for the maintenance of the IT infrastructure based on the policies formulated in discussion with KSCL and based on the industry best practices/frameworks. MSI shall also create and maintain adequate documentation/checklists for the same.

vi. MSI shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, other devices, etc. MSI shall be required to set up the directory server. Logs relating to access of system by administrators shall also be kept and shall be made available to KSCL on need basis.

vii. MSI shall implement a password change mechanism in accordance with the security policy formulated in discussion with KSCL and based on the industry best practices/frameworks like ISO 27001, ISO 20000 etc.

viii. The administrators shall also be required to have experience in latest technologies so as to provision the existing and applicable infrastructure on a requirement based scenario.

c. System Administration

i. 24*7*365 monitoring and management of the servers in the DC.

ii. MSI shall also ensure proper configuration of server parameters and performance tuning on regular basis. MSI shall be the single point of accountability for all hardware maintenance and support the ICT infrastructure. It should be noted that the activities performed by the MSI may be reviewed by KSCL.

iii. MSI shall be responsible for operating system administration, including but not limited to management of users, processes, preventive maintenance and management of upgrades including updates, upgrades and patches to ensure that the system is properly updated.

iv. MSI shall also be responsible for installation and re-installation of the hardware(s) as well as the software(s) in the event of system crash/failures.

v. MSI shall also be responsible for proactive monitoring of the applications hosted

vi. MSI shall appoint system administrators to regularly monitor and maintain a log of the monitoring of servers to ensure their availability to KSCL at all times.

vii. KSCL shall undertake regular analysis of events and logs generated in all the sub systems including but not limited to servers, operating systems etc. The system administrators shall undertake actions in accordance with the results of the log analysis. The system administrators shall also ensure that the logs are backed up and truncated at regular intervals. MSI shall refer to CERT-In Guidelines so as to ensure their alignment with the practices followed.

viii. The system administrators shall adopt a defined process for change and configuration management in the areas including, but not limited to, changes in servers, operating system, applying patches, etc.

ix. The system administrators shall provide hardening of servers in line with the defined security policies. Validation of hardening configuration will be carried out quarterly and deviations must be tracked through SLA reporting

x. The system administrators shall provide integration and user support on all supported servers, data storage systems etc.

xi. The system administrators shall be required to trouble shoot problems with web services, application software, server relationship issues and overall aspects of a server environment like managing and monitoring server configuration, performance and activity of all servers.

xii. The system administrators should be responsible for documentation regarding configuration of all servers, IT Infrastructure etc.

xiii. The system administrators shall be responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of server problems as prescribed in Service Level Agreement.

xiv. The administrators will also be required to have experience in latest technologies so as to provision the existing and applicable infrastructure on a requirement based scenario.

d. Storage Administration

i. MSI shall be responsible for the management of the storage solution including, but not limited to, storage management policy, configuration and management of disk array, SAN fabric/switches, tape library, etc. It should be noted that the activities performed by the MSI may be reviewed by KSCL.

ii. MSI shall be responsible for storage management, including but not limited to management of space, SAN/NAS volumes, RAID configuration, LUN, zone, security, business continuity volumes, performance, etc.

iii. The storage administrator will be required to identify parameters including but not limited to key resources in the storage solution, interconnects between key resources in the storage solution, health of key resources, connectivity and access rights to storage volumes and the zones being enforced in the storage solution.

iv. The storage administrator will be required to create/delete, enable/disable zones in the storage solution.

v. The storage administrator will be required to create/delete/modify storage volumes in the storage solution.

vi. The storage administrator will be required to create/delete, enable/disable connectivity and access rights to storage volumes in the storage solution.

vii. To facilitate scalability of solution wherever required.

viii. The administrators will also be required to have experience in technologies such as virtualisation and cloud computing so as to provision the existing and applicable infrastructure on a requirement based scenario.

e. Database Administration

i. MSI shall be responsible for monitoring database activity and performance, changing the database logical structure to embody the requirements of new and changed programs.

ii. MSI shall be responsible to perform physical administrative functions such as reorganizing the database to improve performance.

iii. MSI shall be responsible for tuning of the database, ensuring the integrity of the data and configuring the data dictionary.

iv. MSI will follow guidelines issued by KSCL in this regard from time to time including access of data base by system administrators and guidelines relating to security of data base.

v. Database administration should follow the principle of segregation of duties to ensure no single DBA can update production tables/data singularly.

vi. In addition to restrictions on any direct change in Data by any administrator, the Databases shall have Auditing features enabled to capture all activities of administrators.

f. Backup/Restore/Archival

i. MSI shall be responsible for implementation of backup & archival policies as finalized with KSCL. The MSI is responsible for getting acquainted with the storage policies of KSCL before installation and configuration. It should be noted that the activities performed by the MSI may be reviewed by KSCL.

ii. MSI shall be responsible for monitoring and enhancing the performance of scheduled backups, scheduled regular testing of backups and ensuring adherence to related retention policies.

iii. MSI shall be responsible for prompt execution of on-demand backups of volumes and files whenever required by KSCL or in case of upgrades and configuration changes to the system.

iv. MSI shall be responsible for real-time monitoring, log maintenance and reporting of backup status on a regular basis. MSI shall appoint administrators to ensure prompt problem resolution in case of failures in the backup processes.

v. MSI shall undertake media management tasks, including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets (onsite and offsite as per the detailed process finalized by during project implementation phase).

vi. MSI shall also provide a 24 x 7 support for file and volume restoration requests at the Data Centre(s).

g. Network monitoring

i. MSI shall provide services for management of network environment to maintain performance at optimum levels on a 24 x 7 basis. It should be noted that the activities performed by the MSI may be reviewed by KSCL.

ii. MSI shall be responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

iii. MSI shall also be responsible for break fix maintenance of the LAN cabling within DC/ICCC etc.

iv. MSI shall also provide network related support and will coordinate with connectivity service providers of KSCL/other agencies who are terminating their network at the DC/ICCC for access of system.

h. Security Management

i. Regular hardening and patch management of components of the ICCC System as agreed with KSCL

ii. Performing security services on the components that are part of the KSCL environment as per security policy finalized with KSCL

iii. IT Security Administration – Manage and monitor safety of information/data

iv. Reporting security incidents and resolution of the same

v. Proactively monitor, manage, maintain & administer all security devices and update engine, signatures, and patterns as applicable.

vi. Managing and monitoring of anti-virus, anti-malware, phishing and malware for managed resources.

vii. Ensuring 100 percent antivirus coverage with patterns not old more than period agreed on any given system

viii. Reporting security incidents and co-ordinate resolution

ix. Monitoring centralized pattern distribution (live update) and scan for deficiencies

x. Maintaining secure domain policies

xi. Secured IPsec/SSL/TLS based virtual private network (VPN) management

xii. Performing firewall management and review of policies on at-least quarterly basis during first year of O&M and then after at-least on half-yearly basis

xiii. Resolution of calls for security notifications, system alerts, vulnerabilities in hardware/ software and alerting KSCL as appropriate

xiv. Performing patch management using software distribution tool for all security applications including content management system, antivirus and VPN

xv. Providing root cause analysis for all defined problems including hacking attempts

xvi. Monthly reporting on security breaches and attempts plus the action taken to thwart the same and providing the same to KSCL

xvii. Maintaining documentation of security component details including architecture diagram, policies and configurations

xviii. Performing periodic review of security configurations for inconsistencies and redundancies against security policy

xix. Performing periodic review of security policy and suggest improvements

xx. Reviewing logs daily of significance such as abnormal traffic, unauthorized penetration attempts, any sign of potential vulnerability. Security alerts and responses. Proactive measures in the event a problem is detected

xxi. Policy management (firewall users, rules, hosts, access controls, daily adaptations)

xxii. Modifying security policy, routing table and protocols

xxiii. Performing zone management (DMZ)

xxiv. Sensitizing users to security issues through regular updates or alerts – periodic updates/ Help KSCL issuance of mailers in this regard

xxv. Performing capacity management of security resources to meet business needs

xxvi. Rapidly resolving every incident/problem within mutually agreed timelines

xxvii. Testing and implementation of patches and upgrades

xxviii. Network/device hardening procedure as per security guidelines from KSCL

xxix. Implementing and maintaining security rules

xxx. Performing any other day-to-day administration and support activities

i. Other Activities

ii. MSI shall ensure that it prepares configuration manual for OS, appliances, middleware, all tool, servers/devices and all equipment's and the same need to be submitted to KSCL, any changes in the configuration manual need to be approved by KSCL. Configuration manual to be updated periodically.

iii. MSI shall maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements and maintenance.

iv. If the Operating System or additional copies of Operating System are required to be installed/reinstalled/un-installed, the same should be done as part of O&M.

v. MSI should carry out any requisite adjustments/changes in the configuration for implementing different versions of Application Software.

vi. Updates/Upgrades/New releases/new versions: The MSI shall provide from time to time the Updates/Upgrades/new releases/new versions of the software and operating systems as required. The MSI should provide free upgrades, updates & patches of the software and tools to KSCL as and when released by OEM.

vii. MSI shall provide patches to the software as part of IT infrastructure, operating system, databases and other applications.

viii. Software License Management: The MSI shall provide for software license management and control. MSI shall maintain data regarding entitlement for software updates, enhancements, refreshes, replacements, and maintenance.

ix. Data backup/recovery management services

x. All other activities required to meet the project requirements and service levels.

xi. It is responsibility of the MSI to scale up the Operations & Maintenance (O&M) team as and when required to ensure smooth project execution throughout the project duration.

4.9.5 Compliance to SLA

i. MSI shall ensure compliance to uptime and performance requirements of project solution as indicated in the SLA (as per Volume III of RFP) table of RFP and any upgrades/major changes to the ICCC System shall be accordingly planned by MSI for ensuring the SLA requirements.

ii. MSI shall be responsible for measurement of the SLAs at the ICCC System level as well as at the user level with the help of the enterprise monitoring tool on a periodic basis.

iii. Reports for SLA measurement must be produced KSCL officials as per the project requirements.

4.10 Compliance to Standards & Certifications

a. For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, MSI will ensure that the entire Project is developed in compliance with the applicable standards.

b. During project duration, MSI will ensure adherence to prescribed standards as provided below:

#	**Component/Application/System**	**Prescribed Standard**
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation

c. Apart from the above MSI need to ensure compliance of the project with Government of India IT security guidelines including provisions of:

- The Information Technology Act, 2000” and amendments thereof and
- Guidelines and advisories for information security published by Cert-In/MeitY (Government of India) issued till the date of publishing of tender notice. Periodic changes in these guidelines during project duration need to be complied with.

d. While writing the source code for application modules MSI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

- The name of the module
- The date when module was created
- A description of what the module does
- A list of the calling arguments, their types, and brief explanations of what they do
- A list of required files and/or database tables needed by the module
- Error codes/Exceptions
- Operating System (OS) specific assumptions
- A list of locally defined variables, their types, and how they are used
- Modification history indicating who made modifications, when the modifications were made, and what was done.

e. Apart from the above MSI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code

- Proper and consistent indentation
- Inline comments
- Structured programming
- Meaningful variable names
- Appropriate spacing
- Declaration of variable names
- Meaningful error messages

f. Quality Audits

- KSCL, at its discretion, may also engage independent auditors to audit any/some/all standards/processes. MSI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with MSI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.
- MSI should comply with all the technical and functional specification provided in various sections in this RFP document.

4.11 Testing and Acceptance Criteria

a. MSI shall demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. MSI may propose further detailed Acceptance criteria which the KSCL will review. Once KSCL provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by KSCL in mutual agreement with bidder and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

b. The following table depicts the details for the various kinds of testing envisaged for the project:

Type of Testing	Responsibility	Scope of Work
System Testing	✓ MSI	▪ MSI to perform System testing ▪ MSI to prepare test plan and test cases and maintain it. KSCL may request MSI to share the test cases and results ▪ Should be performed through manual as well as automated methods ▪ Automation testing tools to be provided by MSI. KSCL doesn't intend to own these tools
Integration Testing	✓ MSI	▪ MSI to perform Integration testing ▪ MSI to prepare and share with KSCL the Integration test plans and test cases ▪ MSI to perform Integration testing as per the approved plan ▪ Integration testing to be performed through manual as well as automated methods ▪ Automation testing tools to be provided by MSI
Performance and Load Testing	✓ MSI ✓ KSCL / Third Party Auditor (to monitor the performance testing)	▪ MSI to do performance and load testing. ▪ Various performance parameters such as transaction response time, throughput, and page loading time should be taken into account. ▪ Load and stress testing of the Project to be performed on business transaction volume ▪ Test cases and test results to be shared with KSCL ▪ Performance testing to be carried out in the exact same architecture that would be set up for production ▪ MSI need to use performance and load testing tool for testing. KSCL doesn't intend to own these tools ▪ KSCL if required, could involve third party auditors to monitor/validate the performance testing. Cost for such audits to be paid by KSCL
Security Testing (including Penetration and Vulnerability testing)	✓ MSI ✓ KSCL / Third Party Auditor (to monitor the security testing)	▪ Solution should demonstrate the compliance with security requirements as mentioned in the RFP including but not limited to security controls in the application, at the network layer, network, data center (s), security monitoring system deployed by MSI ▪ Solution shall pass vulnerability and penetration testing for rollout of each phase. The solution should pass web application security testing for the portal, mobile app and other systems and security configuration review of the infrastructure. ▪ MSI should carry out security and vulnerability testing on the developed solution. ▪ Security testing to be carried out in the exact same environment/architecture that would be set up for production. ▪ Security test report and test cases should be shared with KSCL ▪ Testing tools if required, to be provided by MSI. ▪ During O&M phase, penetration testing to be conducted on yearly basis and vulnerability assessment to be conducted on half-yearly basis.

Type of Testing	Responsibility	Scope of Work
		▪ KSCL will also involve third party auditors to perform the audit/review/monitor the security testing carried out by MSI. Cost for such auditors to be paid by KSCL
User Acceptance Testing of Project	✓ KSCL or KSCL appointed third party auditor	▪ KSCL / KSCL appointed third party auditor to perform User Acceptance Testing ▪ MSI to prepare User Acceptance Testing test cases ▪ UAT to be carried out in the exact same environment/architecture that would be set up for production ▪ MSI should fix bugs and issues raised during UAT and get approval on the fixes from KSCL /third party auditor before production deployment ▪ Changes in the application as an outcome of UAT shall not be considered as Change Request. MSI has to rectify the observations.

Note:

a. Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by MSI for testing in its technical proposal. KSCL does not intend to own the tools.

b. MSI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. MSI must ensure deployment of necessary resources and tools during the testing phases. MSI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of MSI to ensure that the end product delivered by MSI meets all the requirements specified in the RFP. MSI shall take remedial action based on outcome of the tests.

c. MSI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked and it should be protected. Detailed process in this regard including security requirement should be provided by MSI in its technical proposal. The process will be finalized with the selected bidder.

d. All the Third Party Auditors (TPA) as mentioned above will be appointed and paid by KSCL directly. All tools/environment required for testing shall be provided by MSI.

e. STQC/Other agencies appointed by KSCL shall perform the role of TPA. MSI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided and the audit is completed in time. The audit needs to be completed before Go-Live of different phases. MSI needs to prepare and provide all requisite information/documents to third party auditor and ensure that there is no delay in overall schedule.

f. The cost of rectification of non-compliances shall be borne by MSI.

4.12 Factory Testing

Success MSI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.MSI has to provide MAF (OEM certificate) where applicable.

4.13 Final Acceptance Testing

The final acceptance shall cover 100% of the KSCL Project, after successful testing by the KSCL; a Final Acceptance Test Certificate (FAT) shall be issued by the KSCL to MSI.

Prerequisite for Carrying out FAT activity:

1. Detailed test plan shall be developed by MSI and approved by KSCL. This shall be submitted by MSI before FAT activity to be carried out.
2. All documentation related to KSCL Project and relevant acceptance test document (including IT Components, Non IT Components etc.) should be completed & submitted before the final acceptance test to the KSCL.
3. The training requirements as mentioned should be completed before the final acceptance test.
4. Successful hosting of Application, NMS and MIS Software.
5. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the KSCL Project supplied components.

The FAT shall include the following:

1. All hardware and software items must be installed at respective sites as per the specification.
2. Availability of all the defined services shall be verified.
3. MSI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
4. MSI shall arrange the test equipment required for performance verification, and will also provide documented test results.
5. MSI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by KSCL.

   Any delay by MSI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of MSI shall be considered appropriately and as per mutual agreement between KSCL and MSI. In the event MSI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and KSCL may mutually agree to redefine the Network so MSI can complete installation and conduct the Final Acceptance Test within the specified time.

5 Detailed Scope of Work

5.1 Scope of Implementation and Integration components:

5.1.1 Field Equipment: UPS and Others

5.1.1.1 Industrial Grade Outdoor PoE switches

S.N.	Parameter	Minimum Technical Specifications
1	General Features	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100/1000 BASETX access ports, additional 4 x 1000 Base-X SFP & 2x 1GE Uplink ports. One (1) ruggedized single mode SFP should be supplied with the switch.
		The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate
		switching fabric of minimum 16 Gbps or more.
		The switch should support backup storage drives, which will store the last known configuration of the switch, in the case of hardware failure and replacement. Reinserting the storage drive should restore the switch to original working condition without any manual intervention.
2	Layer 2 Features	802. 1Q VLAN on all ports with minimum 10k MAC address
		Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent
		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
		The switch should support IGMP v1/v2/v3 &up to 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.
3	Layer 3 Features	Static, Inter-VLAN routing must be enabled from day one
		The switch should support Dynamic Routing – RIPv1/v2, OSPF for both IPv4 & IPv6, PBR, network address translation etc. protocol by enabling/upgrading the license as & when required.
4	Quality of Service (QoS)	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port
5	Features	The switch should provide traffic shaping and rate limiting features for specified Host, network, Applications etc.
6	Security Features	The switch should support ACLs, Extended IP ACLs, support RADIUS and TACACS+ for access restriction and authentication.

		Should support a mechanism to shut down Spanning Tree Protocol Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
		Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard, DHCP Snooping, DHCP Option 82, Dynamic ARP Inspection (DAI), IP Source Guard, Network Address Translation, BPDU Guard, Port-Security, DHCP Snooping, 802.1x, 802.1AE, MAC Authentication Bypass, 802.1x Multi-Domain Authentication, Storm Control
7	Management Features	The switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
		Support for Automatic Quality of Service or equivalent for easy configuration of QoS features for critical applications.
		Switch should support PTP, FTP/TFTP
8	Mechanical Conditions:	• -5 to +70ºC continuous operating temperature range
		• Operating relative humidity: 5% to 95% no condensing
		Protection Class -minimum IP 30, NEMA TS-2
9	Certifications	Switch should be EN 55022A Class A, VCCI Class A, KN22/CISPR 32 certified
		The switch should support CIP Ethernet/IP, IEEE 1588 PTP.
		EMC interface immunity:
		Switch should be EN55024, EN 61000-4-2 Electro Static Discharge, EN 61000-4-5 Surge, EN 61000-4-8 Power Frequency Magnetic Field, EN 61000-4-11 AC Power Voltage

5.1.1.2 Online UPS – I/2 KVA

S.N.	Parameter	Minimum Specifications
1	Capacity	Adequate capacity to cover all above IT Components at respective location
2	Output Wave Form	Pure Sine wave
3	Input Power Factor at FullLoad	>0.90
4	Input	Three Phase 3 Wire for over 5 KVA
5	Input Voltage Range	305-475VAC at Full Load
6	Input Frequency	50Hz +/- 3 Hz
7	Output Voltage	400V AC, Three Phase for over 5 KVA UPS
8	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9	Inverter efficiency	>90%
10	Over All AC-AC Efficiency	>85%
11	UPS shutdown	UPS should shutdown with an alarm and

S.N.	Parameter	Minimum Specifications
		indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short
12	Battery Backup	Min 2 Hours and as per design consideration
13	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
14	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.
15	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
16	Cabinet	Rack / Tower type

5.1.1.3 Field Junction Box

S.N.	Parameter	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	Powder coated CRCA sheet/ Stainless steel
3.	Material Thickness	Min 1.2mm
4.	Number of Locks	Two
5.	Protection	IP66 / NEMA 4X
6.	Mounting	On Camera Pole / Ground mounted on concrete base
7.	Form Factor	Rack Mount/DIN Rail
8.	Other Features	Rain Canopy, Cable entry with glands and Fans/any other accessories as required for operation of equipment's within junction box.

5.1.1.4 Camera Poles

S.N.	Parameter	Minimum Specifications
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)
2.	Height	5-10 Meters, as-per-requirements for different types of cameras & Site conditions
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)

4.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5.	Bottom base plate	Minimum base plate of size 30x30x15 cm
6.	Mounting facilities	To mount CCTV cameras, Switch, etc.
7.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.
8.	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 in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to earthing standards mentioned elsewhere in the RFP.
9.	Protection	Lightning arrester at select sites as per the requirements
10.	Sign-Board	A sign board describing words such as “This area under surveillance” (in English and Hindi)

5.1.1.5 Junction Boxes

The junction box shall be fitted in secure locations (not easily accessible to the general public) and shall be fitted with a standard cabinet lock. Roadside cabinets shall be secured with anti-tamper fixings in addition to the standard cabinet lock.

- Each Junction box shall be fitted with sufficient screw type terminals to terminate all pairs used and unused. The terminal blocks shall be certified for use with the box.
- Each box shall be equipped with certified cable glands/plug and with earthing bar.
- Cable continuity shall be through junction box dedicated terminals.
- Junction box shall be weather proof to IP 65 as minimum.

5.1.2 Command Control & Communication Centre (ICCC / ICCC)

5.1.2.1 Command Control and Communication Centre Application :

It is envisaged that the city will implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are-

- Smart Parking
- Smart Traffic Management
- Smart Energy Metering
- Smart Water Metering
- Public Safety and Safe City Operations
- Connected Public Transport
- Public Wi-Fi and Urban Service Delivery over Public Wi-Fi
- Environmental Monitoring
- Smart Waste Management

ICCC Platform should comply with following Functional and technical requirements:

S.N.	Description	
1.	Data integration platform of aggregation of	The City will be using various device vendors for various urban services. Various Solutions and technologies of smart elements will be used for deployment and each will be generating data in their own format. This Smart City

S.N.	Description	
	information in form of data	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. Application development and analytics applications should be able to use of various data formats. Open platform to normalize the data to provide secure access to that data using data API(s) to application developer. This data must be exposed to all type of application eco system using secure APIs. The attributes of the API key(s) must restrict / allow access to relevant data from specified domain, sensor, solution identified The platform should be open/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 be open and allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software. The Command & Control solution should adhere to the principles & guidelines of open standards published by GoI. Platform should have fault tolerance, load balancing and high availability. Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion. The platform should be able to convert the data coming from different devices of same type for correlation between various sources.

S.N.	Description	
2.	Distributed Architecture	The platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control
3.	Device Abstraction method	The platform should neutralize the device data into Things Query Language (the underlying language used to communicate among devices) for M2M communication.
4.	GIS Map Support and Location identifier and mapper	System should support Esri, map box, Open street and other GIS applications. a) Map services and geospatial coordinates: provides the geographical coordinates of various assets and locations of the city b) Geospatial calculation: calculates distance between two, or more, locations on the map Location-based tracking: locates and traces devices on the map and provide real time attributes on map when required. 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.
5.	Service management	Performs service management like ID, EVENT Management etc
6.	Developer Program tools	Middleware ICCC Platform should provide online Developer Program tools that help City to develop / integrate new applications, and/or use solution APIs to enhance or manage existing solution free of cost. For platform support there should be technology labs via an online public facing web interface. These labs should be available 24X7.
7.	API Repository / API Guide	Neutral data APIs should be available for the various solutions implemented to monitor, control sensor and/or actuators to provide functionality to enable app developers to develop apps on this platform. API Repository and user guide should be publically available for other OEM/manufactures to do further development of interfaces with out any cost. Cross collaboration APIs enables contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future) to be provided.

S.N.	Description	
8.	Authentication, Authorization	System should support standard Authentication, Authorization protocols
9.	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform
10	Platform upgrade and maintenance	Facility for securely access the ICCC platform remotely for platform updates / upgrades and maintenance for the given duration. Platform should be able to be deployed on a public cloud for disaster recovery
11	Platform functionality, API Management	Provides secure API lifecycle, monitoring mechanism for available APIs as API management. Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions/type of user Provides role-based access view to applications Historical and real-time data available for big data and analytics at any point of time Enables the City and its partners to define a standard data model for each of the urban services solutions using API's
12	ICCC Operation	The solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable. The solution shall also provide an integrated user interface for all the smart solution elements implemented 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 with clear identification code The solution shall provide the "day to day operation", "Common Operating Picture" and situational awareness to the centre and participating agencies during these modes of operation It shall improve visibility for large and geographically distributed environments It shall provide complete view of all solutions in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine

S.N.	Description	
		It shall provide a uniform, coherent, user-friendly and standardized interface It shall provide possibility to connect to workstations and accessible via web browser, a thin-client interface and remotely when required. Rola based filtering should be allowed. The solution should allow creation of hierarchy of incidents and be able to present the same in the form of a parent-child 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 audit trail of read and write actions performed on the system for RCA when required. The solution should provide ability to extract data in various formats for publishing and reporting. The solution should have functionality to attach reference 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: • anticipation of incident • incident or crisis • recovery
13	Integration capabilities	This platform is expected to integrate various urban services devices at the street level sensors or instruments so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices. Platform should be integrate devices using their APIs in to this platform by writing appropriate integration adaptor.

S.N.	Description	
		Platform should support on the fly deployment, add/modify/removal of Sensors without shut down and auto detect of sensors.
14	Edge Computing support for future	Ability to support standard edge appliance to connect industrial protocol devices, provides secure connection deployed infrastructure. Provides remote lifecycle management including software/firmware downloads and upgrades, provides remote management, self-registration, and local administrative interface. ICCC platform should support edge computing where, local processing of events, contextualization, transformation, analytics, decisions and controls happens on edge device. ICCC platform should allow to set or change the behaviour on the edge through policies. Edge computing should learn the behaviour as analysing the data to create better decisions with time. Share the outcomes with other edges when required. Provide centralized Device Management from sensor. Provide management tools to view, analyze, report on and modify the edge configurations. Edge software should be open to use on any sensors and devices or protocols. Same software blueprint should be deployed and running on all edges. Data and Configurations can be different from edge to edge based on requirement.
15	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.
16	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 based on pre-defined threshold. System should allow Default, Time-based,

S.N.	Description	
		Event-based and Manual override polices creation. For example, an operator might enforce a "Lane close/ Electricity shout down " policy manually based on event System should provision to defines a set of conditions that can be used to trigger an event-based policy
17	Notifications, Alerts and Alarms	System should generate Notification, Alert and Alarm messages based on event, issue that should be visible within the Dashboard and to the respective authority over Mobile App if required. All system messages (notifications, alerts and alarms) should always 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 subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification and any other mode available
18	Users and roles	Users access the platform for various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user should be associated with one or more roles and each role is assigned a certain set of permissions for batter access and responsibility. These roles and permissions define the tasks that a user can perform. Additionally, system should assign one or more locations to each role so that the user can perform tasks at the assigned locations only. The platform should allow different roles to be created and assign those roles to different access control policies. System should support LDAP to be used as an additional data store for user management and authentication.
19	Reports	The platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. System should allow dashboard to generate reports and have provision to add reports in favourites list and have provision to send reports automatically based on predefined rules.

S.N.	Description	
20	Standard Operating Procedure	Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation based on use cases defined as per city and solution requirement Integrated Command & Control Center platform should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface. It should have: Ability to edit the SOP, including adding, editing, or deleting the activities. Ability of automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review. Ability to add comments to or stop the SOP (prior to completion). Ability to define the following activity types: **Automation Activity** – Based on predefined rule and threshold, activity initiates and tracks a particular work flow and select a predefined flow order from the list. **Manual Activity –** Based on the emergency event or any other circumstances activity that is done manually by the owner with details of event **If-Then-Else Activity** - Conditional activity that allows branching based on specific criteria. **Notification Activity** - Activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification. **SOP trigger** - An activity that launches another standard operating procedure
21	Collaboration	The CCC platform should have ability to bring multiple stake holders on to a common voice conference call as a standard operating procedure in response configured events Ability to view on various types of devices like computer, smart phones, tablets or normal phones Ability to create collaboration spaces like virtual meeting

S.N.	Description	
		rooms or chat groups manually and notify the users using phone,sms etc. Ability to configuration of the policy under which such collaboration spaces are created and stakeholders are invited and notified. Ability to bring in multiple stake holders automatically into a common collaboration platform in response to a SOP defined to handle a particular event. The platform should allow stakeholders to share content relevant to the issue in the collaboration space. This content may include text, pictures, video, PDF/DOC/DOCX documents etc. and stakeholders should be able to view the content directly from the collaboration space. The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration space. The platform should allow stakeholders to participate in the web conferencing session using any means. The platform should allow smart city devices (cameras, lights, various sensors etc.) to be added to the collaboration spaces. It should also allow to acquire data from such devices and to control such devices directly from the collaboration space, subject to access privileges for each user and device. The platform should allow stakeholders to invoke a web conferencing session directly from the collaboration space. The web conferencing session should automatically include all stakeholders in the collaboration space. The platform should allow stakeholders to participate in the web conferencing session using any means The platform should allow the stakeholders to access the collaboration spaces, participate in conversations, share content, create web conferences and control smart city devices from any endpoint (smart phones, laptops and

S.N.	Description	
		other computers) and from any network location. Collaboration user should be design for all control users. Collaboration services can be offered over cloud.
22	Analytics Engine	Artificial intelligence-based ICCC 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. Analytics engine should be flexible to integrate with other city and government software applications Solution should be robust, secure and scalable. Data Analytics should have minimum below capabilities; a) Advanced Predictive Analytics b) Ability to integrate with other city and government software applications c) Ability to predict insights consuming data from city infrastructure d) Able to predict with measurable accuracy of at least > 60% or batter Ability to have a visualization platform to view historic analytics Ability to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. a) Connect to a variety of data sources b) Analyze the result set c) Visualize the results d) Predict outcomes Ability to support multiple Data Sources. All standard data sources should be supported from day 1 Able to provide analysis of data from a selected data source(s). Able to define arithmetic and aggregation operations that result in the desired output.

S.N.	Description	
		Able to provide capability to check analysis with multiple predictive algorithms
23	Analytics Engine Visualizations	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: a) Change the graph/visualization type b) Print the graph c) Export the graph d) Narrow down on the value ranges e) Toggle the axis labels f) Integrate with other 3rd party applications seamlessly
24	**Infrastructure components/API 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 keypair 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 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 CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.

S.N.	Description	
25	Performance Monitoring Tool	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 • 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 falls below predefined thresholds • Performance monitoring shall not adversely affect the performance of the platform
26	Database monitoring	• Platform should provide database monitoring tool for DB health checks to monitor o Memory allocation, usage and contention o Disk I/O usage o CPU usage for a particular transition o Number of buffers, buffer size and usage o Active locks and locks contention, including waiting time o Active users and status of their operations o List of users (complete or selected) with their access rights
27	Video Display and integration capabilities	• Integrates with existing cameras and new cameras. Should support multiple video sources from multiple locations. Platform should have no limitation in displaying the number of CCTV video sources • Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence. • Display module should have capability to control multi-screened display wall in sync with operator console • The system should dynamically reduce the bit rate and bandwidth for each stream based on the viewing resolution at the remote location • If the remote station is viewing with 352 x 240 (CIF), the stream to remote viewing location should not be using HD bandwidth, but dynamically should change to lower bandwidth

S.N.	Description	
		• If the remote viewing station is viewing this camera in full screen 1080P, then it should dynamically increase the bandwidth to provide HD experience • Smart City Operations Center should use dynamic channel coverage specifically for video stream function for efficient bandwidth usage for multiple operation center and only transmits video stream required to display on monitor to maximize bandwidth efficiency and should support 20 to 30 camera feeds in single display • Platform shall process and transmit video streams adaptive to each video requests from a display server to optimize network bandwidth usage. • Platform shall be able to transmit video streams in remote locations. • 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

5.1.2.2 Contact Centre/Helpdesk for Integration with Emergency Services

S.N.	Minimum Requirements
1.	The contact center solution shall include VoIP based EPBAX, 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 contact center helpline number.
2.	Solution should be designed for upto 30 agents
3.	IVRS should be modular and scalable in nature for easy expansion without requiring any change in the software.
4.	The contact center solution should 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.
5.	The callers should be able to access the various services through state-of-art centralized integrated Interactive Voice Response System (IVRS).
6.	IVRS should 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.
7.	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.
8.	Solution should provide pre-integration with industry standard IVRS servers and enhance routing & screen pop by passing forward the information. Interactive Voice Response System (IVRS) should - a. play welcome messages to callers Prompts to press and collect DTMF digits b. be able to integrate with backend database for self-service, as and when required c. Offer GUI based tool to be provided for designing the IVR and ACD call flow. d. support VoiceXML for ASR, TTS, and DTMF call flows e. be able to Read data from HTTP and XML Pages be able to run outbound campaigns

9.	Automatic call distribution (ACD) solution should - a. be able to route the call to any remote call center agent using IP phones b. have an ability to queue or hold the call for an agent if none is immediately available c. 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 d. be able to perform prioritized call routing e. be highly available with hot standby and seamless failover in case of main server failure f. support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups g. support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc. h. support call routing based on longest available agent, circular agent selection algorithms i. maintain log of all services offered which can be used for audit and analysis purpose. j. 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 k. allow agents to chat with other Agents or supervisor from the Agent desktop software l. allow supervisor to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop m. support Queuing of calls and playing different prompts depending on the type of call and time in the queue
10.	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.
11.	Solution should have automatic identification of incoming number based on landline and mobile number mapping
12.	Solution should support call recording mapped to incident tickets
13.	Solution should offer customizable agent and supervisor desktop layout
14.	Solution should offer Inbound and outbound capability
15.	Solution should provide facilities for outbound calling list management, and software based predictive or preview dialing
16.	The agent's desktop shall have an application which shall fulfil the following functionalities : ▪ It should provide consistent agent interface across multiple media types like fax, SMS, telephone, email, and web call back. ▪ The agent's desktop should have a "soft-phone" – an application that enables standard telephony functions through a GUI. ▪ It should provide the agents with a help-desk functionality to guide the agents to answer a specific query intelligently. ▪ It should also provide an easy access to agents to previous similar query which was answered successfully. ▪ It should also be possible to identify a request to be a similar request made earlier. ▪ It should be possible for agents to mark a query as complex/typical and put in to database for future reference by other agents. ▪ It should be possible for agents to escalate the query.
17.	System should 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.
18.	Should intelligently and automatically responds to email inquiries or routes inquires with skills based routing discipline to agents
19.	Live data reporting gadgets
20.	Multiline support
21.	Speed dial in IP phones
22.	Solution should provide CTI services such as: ▪ 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 o a caller whose call is being attended by the agent o Call routing facilities such as business rule based routing, skills-based routing etc.
23.	Supervisor Module ▪ The call centre should provide a graphical console application program for the supervisor's workstation. This position shall facilitate the following features:- o Any supervisor shall be able to monitor or control any group in the call Centre o 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. o Supervisor console shall also graphically display live status of the call session summary, number of call waiting in the queue, call traffic etc. o Live status of the group shall be shown, including waiting calls and calls being answered currently. o Access to the supervisor console shall be restricted. o It shall be possible for a supervisor to attend calls whenever necessary.
24.	Reporting: ▪ System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc. ▪ 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.
25.	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 must be logged. ▪ System shall have at a minimum following standard reports: o List of users, user privileges and status o User sign-off and sign-on o User violation – unsuccessful logon attempts o User additions, amendments and deletions with before & after image

5.1.2.3 Video Display Wall (VDM)

S.N.	Perameters	Minimum Technical Specification

1	Size	70” (70 Inches diagonally) or more with complete configuration of (5 cubes x 2 cubes) with covered base. All cubes have to be of the exactly same size, configuration
2	Resolution	Full high definition (1920 x 1080); aspect ratio of 16:9 Widescreen with LED/laser light source in redundancy
3	Contrast Ratio	Dynamic contrast should be min 1,000,000:1 or better
4	Colour & Brightness	Minimum 250 nits and should be adjustable for lower or even higher brightness requirements Uniformity: >=95% or batter Uniform brightness and colour. The colour calibration should be automatic and continuous operations for 24x7 operation
5	LED Life	The light source lifetime of the LED shall be at least 90,000 hours. This should be certified by the OEM.
6	Placement	The inter screen gap (bezel gap) should be <0.4 mm or batter and viewing angle Should be 178 degree/178 degree (H/V)
7	Dust Prevention	Should be designed to avoid dust / Dust tight and resistant / Follow standards as prescribed by Government
8	Input & Control	Analog D-sub/Ethernet/Digital DVI/Digital HDMI and VGA input with On Screen Display (OSD) and IR remote control
9	Display	shall provide image uniformity across the whole display area, real-time clear luminous view to share information between operators and decision makers, flicker free image on the Large Screen for seamless display
10	Capability	Ability to displaying high definition (HD) and standard definition (SD) content., Low maintenance

5.1.2.4 Video Wall Controller

S.N.	Parameters	Minimum Technical Requirements
1	Display controller	Controller to be able to control min 8 cubes and Controller to control Video wall in a matrix arrangement as per design and redundant for high availability and support Minimum1920 x 1080 or higher
2	Platform	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery
3	CPU	Min 16 GB RAM with Quad/Octa Core processor (3.4 Ghz) or higher and Redundant Hot Swappable HDD in RAID 1 Configuration
4	Chassis Type	19" Rack mount industrial chassis with adequate cooling fans and power supply on higher availability in hot swappable
5	Network	Min 2 Network Ports and more
6	RSS Feed	The controller should be able to show the RSS feed as required
7	Scalability	The system should be able to add additional inputs as required in the future

8	Keyboard & Mouse Extension	Keyboard and Mouse along with extendable mechanism up to display.
9	24 x 7 operation	The controller shall be designed for 24 x 7 operation and high availability
10	Others	The Video Wall and the Controller should be of the same make to ensure better performance and compatibility

5.1.2.5 Video Wall Management Software

S.N.	Parameters	Minimum Specification
1	Display & Scaling	Displaymultiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows 3Ability to input, manage, and distribute visual content, including digital CCTV video, web pages, CATV, workstation applications, and active screens from any networked/remote workstation.
3	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 wall in any size. Ability to stretch, re-position, and resize any video source on any display device. Ability to treat the VDW as a single display. It shall act as a single canvas with no pixel separation.
4	Other features	• SMTP support, Remote Control over LAN or VPN • Ability include an administrator role that shall be able to manage system configuration, sources, user groups, and user authentication. • Alarm, Remote and Multiple concurrent client • Ability to commands on wall level or cube level or a selection of cubes : • Switching the entire display wall on or off. • 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. • Fine-tune colour of each cube • KVM Support and GUI

5.1.2.6 Monitoring Workstations

S.N.	Parameters	Minimum Requirements
1	Processor	Latest generation 64bit x 86 Xeon Processer with latest chipset
2	Motherboard	OEM Motherboard
3	RAM	Minimum 8 GB DDR3 RM expendable to 32 GB
4	Graphics card	Minimum Graphics card with 2 GB video memory (non-shared)

5	Monitor	Monitors of 24" TFT LED monitor, with Minimum 1920 x1080 resolution, Minimum input of 1xDP, 1x HDMI, 1xDVI, Energy star 5.0/BEE star certified
6	HDD	Min. 1 TB Hard Drive @7200 rpm
7	Other Accessories	Line/Mic IN, Line- out/Spr Out (3.5 mm), Minimum 6 USB ports (out of that 2 in front), 104 keys minimum OEM keyboard, USB Optical OEM mouse,
8	PTZ joystick controller	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
9	Operating System	64 bit pre-loaded OS with recovery disc
10	Antivirus feature	Advanced antivirus, antispyware, desktop firewall and encryption as required.

5.1.2.7 Desktops for Helpdesk

	Parameters	Minimum Technical Specifications
1.	Processor	latest & high performance (3.0 Ghz) or higher
2.	Memory	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade
3.	Motherboard	OEM Motherboard
4.	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher
5.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)
6.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port
7.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/
8.	USB Ports	Minimum 4 USB ports
9.	Display Port	Minimum 1 Display Port (HDMI/VGA) port
10.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.
11.	Mouse	Optical with USB interface (same make as desktop)
12.	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified.
13.	Operation System and Support	Pre-loaded Windows 10 (or latest) Professional 64 bit, licensed copy All Utilities and driver software, bundled in CD/DVD/Pen-drive media.
14.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified

5.1.2.8 Ceiling Speakers

- 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.
- 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 either in-built noise sensors with the ceiling speakers or an independent ambient noise monitoring system.

5.1.2.9 IP Phones

#	**Parameter**	**Minimum Specifications**
1.	Display	2 line or more, Monochrome display for viewing features like messages, directory
2.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface
3.	Speaker Phone	Yes
4.	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5.	VoIP Protocol	SIP V2 VoIP supported
6.	POE	IEEE 802.3af or better and AC Power Adapter (Option)
7.	Supported Protocols	SNMP, DHCP, DNS
8.	Codecs	G.711, G.722, G.729 including handset and speakerphone
9.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/off button, microphone mute
10.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
11.	Phonebook/ Address book	Minimum 100 contacts
12.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13.	Clock	Time and Date on display
14.	Ringer	Selectable Ringer tone
15.	Directory Access	Able to integrate with LDAP standard directory
16.	QoS	QoS mechanism through 802.1p/q

5.1.2.10 IP PBX (Call Control System)

#	**Minimum Specifications**
3.	The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture
4.	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity
5.	The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted
6.	The voice network architecture and call control functionality should be based on SIP
7.	The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.
8.	The communication server and gateway should support IP V6 from day one so as to be future proof
9.	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM
	Support for call-processing and call-control
10.	Should support signaling standards/Protocols – SIP, MGCP, H.323, Q. Sig
11.	Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC
12.	The System should have GUI support web based management console Security
13.	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
14.	System should support MLPP feature
15.	Proposed system should support SRTP for media encryption and signaling encryption by TLS
16.	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
17.	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
18.	Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.

5.1.2.11 Video Conferencing Unit

#	**Parameters**	**Minimum Specifications**
1	Protocols	The system should be able to call any H.323 and SIP endpoint directly or indirectly. It should be possible to share content via BFCP and H.239 Endpoint should support the latest video coding standard eitherH.263, H.264, H.265 It should support Audio coding G.722, G.722.1, G.711
2	Network	Endpoint should support bit rate up to 8 Mbps or more on IP (H.323and SIP) Minimum 2 X Gigabit Ethernet: Should support 10/100/1000 BASET
3	Main Video Resolution	Shall work in high definition video resolution of 1080p 60fps for live video for both Transmit and receive
4	Camera	Inbuilt in the Integrated system with 2 cameras Both cameras should be capable of automatic voice tracking capability so as to automatically zoom and focus on to the person speaking in the room.

		Zoom: Minimum 10x (optical) or better
5	Video Inputs	Minimum 3 HDMI inputs and 1 DVI input for connecting PC / laptop
6	Video Outputs	Minimum 2 x HDMI or similar or better to connect two displays. Additional Outputs are desirable.
7	Audio Inputs	It should support minimum 7 Omnidirectional / Directional Microphones. 3 microphones to be supplied from day one with the system.
8	Encryption	AES 128 bit or more, TLS, SRTP, HTTPS or similar or better
9	User Interface	Intuitive touch panel to operate the entire system

5.1.2.12 Multiparty Conference Unit (Video and Audio Conferencing Bridge with Secure VC over Internet)

#	**Minimum Requirements**
1.	The Bridging should be running on the standard servers on standard Virtualized platforms. The hardware, software and virtualization software should be supplied and supported by a single vendor.
2.	From day one the bridge must provide 6 full HD video ports @1080p 30 fps and 30 audio conference ports.
3.	All necessary hardware to support the above capacity needs to be supplied from day one. Bridge must have a redundant power supply.
4.	All the ports must be able to connect different sites at different bandwidths and protocols.
5.	H.264 AVC standard must be supported at the minimum to connect all the sites.
6.	The bridge should support room based video end points, users joining from browsers’ supporting WebRTC and HTML5 and its own clients. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution.
7.	The bridge should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies.
8.	The bridge should have components such as the Web Server for Web RTC, Scheduler as part of the offering from day one.
9.	Should support H.261, H.263, H.263+, H.263++, H.264, WebRTC video algorithms.
10.	Should support video resolution from SD to Full HD to join into a conference.
11.	Along with the Support for basic algorithms like G.711 and G.722.1 the bridge should also support wideband Audio protocols like MPEG 4 AAC - LC and MPEG 4 AAC – LD.
12.	Must support the ability to allow Video conferencing devices, Clients on Mobile phones, Smart phones and Laptops to join into conference. These clients can be inside the WAN network or even on the Internet without a VPN.
13.	The bridge should support transcoding of different Audio/video Protocols.
14.	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).
15.	The bridge must also support advanced continuous presence such that the site that is "on-air" to be seen on a larger window and the other sites are seen in smaller quadrants.
16.	The bridge must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM.
17.	The bridge should support 128 Bit strong AES encryption for calls and H.235 for authentication.

#	Minimum Requirements
18.	It should be possible for outside agencies (for state government, central government, police department, etc.) to join the bridge for multi-party video conference call securely over internet.
19.	They should be able to join the bridge using standards based VC endpoints using internet (as long as these endpoints are exposed to internet) securely.
20.	It should be possible to connect 5 such external endpoints / locations concurrently at any given point of time.
21.	It should use secure firewall traversal technology.
22.	It should support any standards-compliant SIP or H.323 video conferencing endpoints.
23.	It should support for H.323 SIP Interworking Encryption and H.323 SIP Interworking DuoVideo.
24.	It should use standards based firewall traversal methods - H.460.18/19.

5.1.2.13 Fixed Dome Camera for Indoor Surveillance

Refer Specification of fixed camera in CCTV surveillance section 4.3.2.4

5.1.2.14 Non-IT Requirements , Specifications & Office Interior Spaces

The selected bidder should adhere to the specifications given below for Non-IT components. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centre and Office premises before Go-Live.

General Standards:

The ICOMC 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.

5.1.2.14.1 Civil and Architectural Work

False Ceiling:

Metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.

Minimum 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 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. All workstations, cabins should be as per industry best practices and standards.

Providing & making of 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 polish

An 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 fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size min. 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. Glazing including the framework of 4" x 2" powder coated aluminium 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.

Flooring (wherever required as per approved drawing)

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:

1. Point of Load (PoL) shall be considered 20% more than the actual load

2. Uniform Distribution Load shall be calculated according to the final Point of Load
3. Noise-proof, Fireproof
4. Maintenance window for easy access to under the raised floor
5. Separate electrical and data cable tray under the raised floor
6. Face of floor tiles shall conform to the aesthetic part of the approved design
7. 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.

Air Conditioning and Natural Convection

For Data Centre -

Precision remote control and manual operated air conditioning system shall be exclusively installed to maintain the required temperature in the data center server farm area. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. Air conditioner shall be linked to secondary power supply as well to prevent them from shutting down in case of power outage

Painting

Provide and apply 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 and fire line gyp-board ceiling.

Use approved fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.

5.1.2.14.2 PVC conduit:

The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for non- metallic 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.

5.1.2.14.3 <u>Wiring</u>

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. Looping system of wring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations.

Wherever wiring is run through trunking 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 where required

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.

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.

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.

5.1.2.14.4 <u>Cable Work</u>

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. Cable shall be laid as per the IS standard

All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers should be properly punched. 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.

5.1.2.14.5 Fire Detection and Control Mechanism

Fire can have disastrous consequences and affect operations of a Control Room. It is required that there is early-detection of fire for effective functioning of the Control Room. The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards.

- Should proactively alert incase there is a possibility of a electrical fire (short circuit or over current)
- The system should have the capability to integrate with different makes of fire alarm systems in the DCs and provide the alarms generated by the system on the centralized Dashboard.
- The system should be able to plan and process a proper evacuation plan incase of fire
- Trigger Audio and Visual alarm
- Co-relate with the nearest camera in the site with the zone of the FAS.
- Switching ON of lights on the evacuation pathway.

5.1.2.14.6 Rodent Repellent System

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, nontoxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However MSI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

5.1.2.14.7 Access Control System

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. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for 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 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:

#	**Description**
1.	Controlled Entries to defined access points
2.	Controlled exits from defined access points
3.	Controlled entries and exits for visitors
4.	Configurable system for user defined access policy for each access
5.	Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
6.	User defined reporting and log formats
7.	Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
8.	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.

5.1.3 Smart City Data Centre

MSI has to implement City Datacentre to cater the requirements of Data compute, storage and for city analytics purpose.

5.1.3.1 ICT Hardware Components for Data Centre

5.1.3.1.1 Internet Router

#	**Item**	**Minimum Technical Specifications**
1.	General	Core router shall be chassis based with modular architecture for scalability with Redundant - Route Processor, Power supply, Switching fabric; and shall deliver multiple IP services over a flexible combination of interfaces.
		The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT),capability. The router should also support hitless interface protection, In-band and out-band management, Software rollback feature, Graceful Restart, non stop routing for OSPF, BGP, LDP, MP-BGP etc.
		The platform shall have modular software that will run service & features as processes having full isolation from each other

#	Item	Minimum Technical Specifications
		Router shall have event and system history logging capabilities. Router shall generate system alarms on events and capable of log analysis
		Router should have power supply redundancy. There should not be any impact on the router performance in case one of the power supplies fails.
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with 6 x 1 GE port with required transceivers as per solution & one 10 gig interface.
3.	Interface modules	▪ Should support minimum 1G/10G/40G interfaces ▪ Must have capability to interface with variety interfaces
4.	Protocol Support	▪ The router shall have RIPv1, RIPv2, RIPng, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation)
		▪ Tunneling with 1000 tunnels enabled from day one. ▪ Router should support following MPLS features – LDP, Layer 2 VPN such as EoMPLS with LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled from day one. Support for these features can be considered optional for Internet routers
5.	Manageability	The router must support management through SNMPv1/v2/v3, support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring & deep and stateful packet inspection to recognize a wide variety of applications The router shall be provided with IETF standards based feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA operations shall provide information on TCP/UDP delay, jitter, application response time, Packet Loss etc
6.	Scalable	The router should be scalable. For each slot multiple modules should be available. The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.
7.	Traffic control/QoS	The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques. The router shall support QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QOS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non-congestion scenario.
8.	Bandwidth & Performance	Backplane Architecture: The back plane architecture of the router must be modular and redundant. The back plane bandwidth must be minimum 20 Gbps from day one with minimum scalability upto 30 Gbps with minimum routing performance of 20 mpps form day one (1) scalable upto 30 mpps, with minimum three (3) open slots.
9.		The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability. The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.

#	Item	Minimum Technical Specifications
10.	Redundancy	▪ Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis ▪ All interface modules, power supplies should be hot- swappable
11.	Security features	The router should have support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT) . The router shall support NAT6to4 function. Mention the number of sessions that it can support. The router shall support vrf-aware NAT function. The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc. Router should support deep and stateful packet inspection to recognize a wide variety of applications. The router shall support firewall service in hardware on all interfaces for enhanced security to protect the backbone from malicious activities. The firewall performance shall be at least 5 Gbps (internal/external). In case of external firewall, bidder should propose the firewall with necessary 10G interface and redundant power supply.

5.1.3.1.2 Next-generation Firewall with IPS and anti-APT

#	Perameters	Minimum Technical Specifications
1	**Hardware Architecture**	The proposed solution/appliance MUST be upto Layer 7 protection. There should be no performance degradation in the overall transaction processing. The solution shall be deployed in HA mode in the DC/ICCC.
		The appliance based security platform should be capable of providing firewall, application visibility, and control, VPN functionality in a single appliance.
		The proposed firewall appliance should have at least 12 ports of 10/100/1000 and minimum 4 ports of 10 Gig SFP+ ports with separate management and 2 * 40 G ports from Day one and should be scalable to more 2 * 40G ports in future
		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats. The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory
		The proposed solution should have dual redundant power supply and redundant hot swappable fans.
		Firewall Should consume 1RU Form Factor.
2	**Performance & Scalability**	Should support at least 10 Gbps NGFW throughput under real world production Conditions. This throughout should include FW,IPS/Threat Prevention and AVC.
		Should support minimum 5 Gbps of IPSec VPN throughput.
		Firewall should support at least 8 Million concurrent sessions with AVC feature turned on.
		Firewall should support at least 65,000 connections per second with AVC feature turned on.
		Firewall should support at least 1000 VLANs
3	Next Generation Firewall Features	Firewall should provide application detection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP
		Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously

		Firewall should support operating in routed & transparent mode
		Should support Static, RIP, OSPF, OSPFv3 and BGP
		Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
		Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
		Firewall should support Multicast protocols like IGMP, PIM, etc
		Should support security policies based on security group names in source or destination fields or both
		Should support capability to limit bandwidth on basis of apps / groups, Networks / Geo, Ports, etc
		The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).
		The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
		The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
		Should support Application Visibility and Control (AVC) supports more than 10000 application-layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.
		Proposed appliance should also provide Reputation- and category-based URL filtering offers comprehensive alerting and control over suspect web traffic and enforces policies on hundreds of millions of URLs in more than 50 categories
		The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
		The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.
		The solution shall provide on-premise based sandbox technology where the objectionable content may be executed and inspected. Local Malware analysis appliance should have integrated redundant power supply and minimum of 2 x 10 ports
4	High-Availability Features	NG Firewall should support Active/Standby failover.
		Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for provide additional level of redundancy
		Firewall should support redundant interfaces to provide interface level redundancy before device failover
		Firewall should support 802.3ad Ether channel or equivalent functionality to increase the bandwidth for a segment.
5	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software

		The management platform must provide a highly customizable dashboard.
		The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
		The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
		Should support REST API for monitoring and config programmability
		The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
		The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
		The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
		The management platform must risk reports like advanced malware, attacks and network
		The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

5.1.3.1.3 Gateway level anti-virus and anti-spam security solution

#	Parameters	Minimum Technical Specifications
1	**General**	The solution should provide a comprehensive email security solution that integrates against inbound and outbound, Internal defences against email threat such as spam, virus, etc. Solution should cater to minimum 2,000 User. The solution shall be hardware appliance based.
		The solution should be appliance based. Appliance should support ant-spam, anti-virus(can support 2 different engine), outbreak filter , on appliance detail reporting and on- appliance quarantine handling. Same appliance should have provision to run Advance malware protection for future requirements.
		The appliance based Solution should be provided with Proprietary Operating System and MTA on appliance and not open source operating system (sendmail, qmail or postfix) .
		Appliance should have 1.8 TB hot swapable HDD and RAID support
		Appliance should have atleast 2 hexa core processor and 32 GB RAM
		The solution should have performance capability of processing at least 1,00,000 message per hour. The salutation should support at least 4 * 10/100/1000 copper interface. Appliance have option for 10G interface if require
		Appliance have option for DC power, if require
		The solution should be IPV6 ready
		The solution should be protect Directory Harvesting attacks.
		The solution should support LDAP integration and synchronization .LDAP integration should be used defining policies and when delivering mails.

#	Parameters	Minimum Technical Specifications
		The solution should support multiple email domains on the same system for each domain a specific destination mail server can assigned for delivery.
		The solution should be supplied including all hardware, accessories, license, software with pre-hardened operating system. Hardware should be from same OEM
2	Inbound SMTP Protection (SPAM)	The solution should combine sophisticated content based Anti-Spam technology ,IP reputation and RBL to effective block spam
		The solution should accurately filter/detect more than 99% of spam
		The solution should support email authentication using SPF (Sender Policy Framework).
		The solution should support Domain Key Identified Mail(DKIM) verification of email messages.
		The solution should support lookup to the cloud to perform sender, message and IP reputation to effectively block spam.
		The solution should support defining custom bypass for the sender IP for the IP reputation.
		The solution should support anti-relay. It should have capability to configure domain to which to solution accept or refuse mail.
		The solution should support RBL lookup .It should support adding of multiple RBL list.
		The solution should have an option to block mail by sender domain address .
		The solution should have an option to block mail by sender email address.
		The solution should support scouring or signature to detect spam. Based on a severity a different action should be configured .
		The solution should support anti-phish scanning.
		The solution should offer various action offers for spam detect such as monitor, block, quarantine, forward etc.
3	Anti virus Protection	The solution should proposed contain a network level solution for the SMTP traffic.
		The solution should have ability to block Malware etc.
		The solution should protect against mass mailing worm.
		The solution should contain an option to configure scan all file or specific file type.
		The solution should contain an option to scan archive file.
		The solution should have ability to perform reputation analysis. It should ability to send to suspicious file information to the cloud analysis.
		The solution should contain an option to configure the maximum size of attachment file, in case size is exceeds the antivirus solution block all or pass all files.
		The solution should contain an option to configure the maximum nesting level of attachment file. in case size is exceeds nesting level the antivirus solution should block all or pass the file.
		The solution should offer various actions for virus detect clean, quarantine, deliver or forward etc.

#	Parameters	Minimum Technical Specifications
4	Outbound SMTP Protection	The solution should able to monitor and protect mail flowing out of network in SMTP traffic.
		The solution should allow to administrator to automatically add text to outbound mail such as legal disclaimer.
		The solution should perform image based filtering. It's should use sophisticated analytical algorithm to analyse image to determine attributes that indicate the image may be of a pornographic or non-pornographic nature.
		The solution should contain an option to configure maximum message size. In case message size exceed the mail should be blocked or quarantine.
		The solution should contain an option to configure maximum attachment size. In case attachment size exceed the mail should be blocked or quarantine.
		The solution should support file category/file extension wise filtering/blocking. Categories should include document, database, multimedia, archive etc.
		The solution should support handling of encrypted content.
		Appliance should support Tamplate based DLP on the same appliance with enabling single license. Not require any additional appliance for the same.
		Appliance should support Email encryption on the same appliance with enabling a single license
5	Policy Creation & Management	The solution should provide granular policy for Inbound, Outbound and Internal traffic.
		The solution should be able to create specific policy based on. 1. Source/Destination IP address. 2. Sender/Recipient email address. 3. Alias recipient email address list. 4. LDAP user group. 5. Masquerade sender email address The solution should be able to create specific policy message security such as TLS
6	Email Management	The solution should able to manage the email in the message queue though the GUI.
		The solution should able to view the status of all messages in the queue for the GUI.
		The solution should able to filter and view message that was: 1. Block,2.Bounced,3.Delivered,4.Quarantined,5.Queued
		The solution should able to filter and analyse message using: 1. sender,2.Reciepent,3.Subject,4.Inbound/Outbound,5.Date,6.Source IP
		The solution should offer a wide range option to the message in the queue such as Delete, Retry, Forward, etc.
		The solution should support end-user quarantine. Is it with buttons 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.
		The solution should support on box quarantine or dedicated quarantine appliance.

#	Parameters	Minimum Technical Specifications
		The solution should have configurable retention period for spam email or events.
7	System Administration	The solution should support restricted access to the system for management though SSH/web GUI. Administrator should able to specify a list of authorize access.
		The solution should provide the real-time health status of all modules on the dashboard for CPU, memory utilization, total number of concurrent connections etc.
		The solution should automatically backup all configurations on the system at specific time.
		The solution should offer various built in report etc. 1. Overall message summary 2. Inbound message summary 3. Outbound message summary 4. Spam and virus summary 5. Message transfer summary 6. System capacity The solution should offer alerting capabilities, including e-mail and SNMP/SIEM
		The solution should be automatically security update .Vender should provide update and security enhancement to operating system, MTA, and supporting software include antivirus and antispam engine.
		The solution should able to generate report in PDF/HTML/Other Format.
		The solution should support inbuilt troubleshooting tools to troubleshoot issue. i.Built-in command to consolidate diagnostic information and configuration and send to customer support ii. Ability to enable remote tunnel support for remote diagnosis

5.1.3.1.4 Network Behaviour Analysis

#	Minimum Specifications
1	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.
2	Should capture signature / heuristics based alerts and block the same
3	Should Identify the source of an attack and should not block legitimate users
4	Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities
5	The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc.
6	Should be capable of conducting protocol analysis to detect tunneled protocols, backdoors, the use of forbidden application protocols etc.
7	Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.

#	Minimum Specifications
8	The solution should Integrates with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format
9	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS
10	Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue
11	The system should be able to monitor flow data between various VLANS
12	Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.
13	Should support the capability to link usernames to IP addresses for suspected security events.
14	Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.
15	Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer
16	Solution should be compatible with a virtual environment.
17	The solution should provide access to raw as well as processed logs
18	Dashboard should have the facility to be configured according to user profile
19	System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues
20	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.
21	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.
22	Solution should support ubiquitous access to view all reporting functions using an internet browser.
23	The solution should support the identification of applications tunnelling on other ports
24	Solution should be able to collect security and network information of servers and clients without the usage of agents
25	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance
26	The solution should have the ability to statefully reassemble uni-directional flows into bidirectional conversations; handling de-duplication of data and asymmetry
27	The solution should support all forms of flows including but not limited to cisco netflow, juniper jflow, sflow, ipfix for udp etc.
28	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record

#	Minimum Specifications
29	The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address
30	The solution should be able to leverage external threat feeds for information about known CnC connections, botnets, Tor exit nodes, etc.
31	Network performance
32	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.
33	Solution should probe the network in a manner so that impact on network performance is minimal.
34	Should support both in line and offline modes.
35	The tool should have a system for interactive event identification and rule creation
36	Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.
37	Solution should have facility to assign risk and credibility rating to events.
38	Solution should support traffic rate up to 1 Gbps

5.1.3.1.5 Web Security Appliance

#	Parameter	Minimum Technical Specifications
1	Appliance Requirement and Functionality	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.
2	Hardware	Minimum of 1 * 6-core CPUs, 2.4 TB storage, RAID 10, 32 GB or more DRAM, hot-swappable hard drive
3	Operating System	The appliance based Solution should be provided with hardened Operating System.
4	Operating System Performance	The underlying operating system and hardware should be capable of supporting atleast 2000 users from day with licenses & scalable upto 5000 users.
5	Operating System Security	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.
6	Forward proxy mode	The solution should support explicit forward proxy mode deployment in which client applications like browsers are pointed towards the proxy for web traffic.
7	Transparent mode	The solution should also support transparent mode deployment using WCCP v2 and L4 switches/PBR (Policy based Routing)
8	Pac File support	The appliance should support hosting proxy auto-config files that defines how web browsers can automatically choose the appropriate web proxy for fetching a URL.
9	Support multiple deployment options	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.

#	Parameter	Minimum Technical Specifications
10	Proxy Chaining	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies
11	DNS Splitting	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain
12	IP Spoofing support in transparent mode deployments	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.
13	High Availability	Provision of active/active High Availability is required
14	Proxy support	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.
15	HTTPS Decryption	The solution should support HTTPS decryption
16	HTTPS decrypted traffic scanning	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.
17	HTTPS decryption policy	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action
18	File download and size restrictions	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.
19	IP based Access Control	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's
20	User based Access Control	The solution should support integration with active directory and/or LDAP. This should allow administrator to define user or group based access policies to Internet
21	Multiple Authentication Server Support	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.
22	Application and Protocol Control	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.
23	Layer 4 Traffic Monitoring	Should detect Phone Home attempts occurring from the entire Network. It should support actions to allow traffic to & from known allowed & unlisted addresses & block traffic to & from known malware addresses & should support monitoring suspected malware addresses.

#	Parameter	Minimum Technical Specifications
24	Bandwidth restrictions	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.
25	Anti Malware	The appliance should support at least 2 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Keyloggers and as defined by the organizations policy. Please mention the antimalware engine.
26	Anti-Malware	With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.
27	Web Reputation	The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.
28	Customizable Web Reputation	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.
29	Incoming/Outgoing Traffic scanning	The solution should scan for Incoming and outgoing traffic.
	Outbound connection control on all ports and protocols	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively
		mitigate malware that attempts to bypass Port 80
30	Custom URL filtering	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organisation.
31	Url Filtering Options	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.
32	Dynamic Categorization	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.
33	Reporting Mis-categorization	The solution should have facility for End User to report Mis-categorisation in URL Category.
	URL check & submission	Support portal should give facility to end user to check URL category and submit new URL for categorization
34	Filtering Content	Solution should support filtering adult content from web searches & websites on search engines like Google.
35	Signature based	The solution should support signature based application control.

#	Parameter	Minimum Technical Specifications
	application control	
	End User Notification	Solution should support following end user notification functionalities.
		The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.
		When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.
		The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.
		Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organisation is monitoring their web activity.
36	Remote support	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.
37	Secure Remote Access	The Support Engineers should be able to login to appliance using secure tunnelling methods such as SSH for troubleshooting purposes
38	Diagnostic Tools	The appliance should have diagnostic network utilities like telnet, traceroute, nslookup and tcpdump/packet capture.
39	Updates and Upgrades	The appliance should provide seamless version upgrades and updates.
40	Secure Web Based management	The appliance should be manageable via HTTP or HTTPS
41	CLI based management	The appliance should be manageable via command line using SSH
42	Serial Console access	For emergency, the appliance should have serial console access
43	Ethernet Management	Should have provision for separate Ethernet for managing the appliance
44	Web Logs	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.
45	Retention Period	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP.
46	User Reports	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)
47	Bandwidth Reports	Reports on Bandwidth Consumed / Bandwidth Saved

#	Parameter	Minimum Technical Specifications
48	Detailed logging	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it
49	Blocked by reputation &malware reports	It should support reporting web requests blocked due to web reputation & blocked by malware
50	Report Formats	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.
51	Scheduling of Reports	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.
52	System Reports	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.
53	Updates and Upgrades	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor
54	IP V6 Support	Should have the ability to proxy, monitor, and manage IPv6 traffic.

5.1.3.1.6 Data Centre Core Switch

#	Parameter	Minimum Specifications
1.	Hardware & Performance requirements	Chassis based Multilayer Switch with sufficient modules/line cards to fit required transceivers/UTP ports. Chassis shall have minimum 7 payload slots. The switch must have front to back airflow.
		The total aggregate switching capacity shall be scalable up to 28 Tbps. Per slot throughput should be 3.8 Tbps
		There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, system clock, power supplies and fans etc should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable
		The switch should have redundant CPU's working in an active or active-standby mode. There should not be any traffic disruption during the CPU fail-over/change-over and the fail-over time should be less than 1 sec.
		Should Support Hitless software upgrades to reduce downtime during software upgrade. The switch must support Fault isolation per process and process patching to enhance the switch availability
		The Switch should support non-blocking Layer 2 switching and Layer 3 routing.
		The Backplane should be 100% Passive. Preferably back plane free design to optimize the airflow and power consumption.
		The Switch should have a Truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).
		The switch must support 1/10G SFP+, 1/10 G Base-T and 40G QSFP based port line cards. The switch must scalability to support minimum 200 nos of 40 G QSFP ports or more. Bidder to choose required ports as per their solution.

#	Parameter	Minimum Specifications
		Support for Unidirectional Link Detection Protocol (UDLD) or equivalent, Layer 2 trace route or equivalent to ease troubleshooting
2.	Layer 2 and Layer 3 Functionality	Should support port, subnet based 802.1Q VLANs. The switch should support 4096 vlans. The switch must support Private VLAN or equivalent.
		The switch should support 50K no. of MAC addresses
		Switch must support spine - leaf topology based on VXLAN and create large layer 2 domains.
		Switch must support multi chassis ether channel feature and work with any downstream switch, server from various vendors.
		Should support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection.
		Switch should support virtual routing functionality from day 1
		Should support minimum 32K Route entries for IPv4 and IPv6 routes.
		Switch should support 8K Multicast route
		Switch must support IP v4 – HSRP/ VRRP and IP v6 - HSRP v6/ VRRP v6. It must also support DHCP Relay V4 and V6
3.	Remote Line card and Virtualization support	Switch must support IEEE 802.1BR (Bridge Port Extension) or equivalent technology, which in turn enable remote line card functionality to optimize cabling inside the data center
		Switch must support virtualization features like VXLAN Gateway/Bridging and routing functionality. Capability of supporting NVGRE is preferred.
4.	Minimum Port Requirement from Day 1	Switch should have minimum of 72 x 40G Ports
5.	Compliance/ Certifications	EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program would be preferred

5.1.3.1.7 Data Centre Switches

#	Parameter	Minimum Specifications
1.	Ports	▪ Must have minimum 48 x 1/10 G SFP+ and 6 X 40 G QSFP port, SI to choose required transceivers as per their solution. Core/ Spine to TOR/ Leaf switch connectivity should be at multiple of 40G links.
2.	Hardware features	• Proposed network device must be 19" rack mountable & Maximum 2 RU in size. • It is desirable that the network infrastructure is based on delivering front to back airflow. • Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy and Must have N:1 fan module redundancy. • All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast). • Must be field upgradeable/license upgradeable to Layer 3 for investment protection. • Must have Line-rate traffic throughput on all ports at Layer 2. • Must have Line-rate traffic throughput on all ports at Layer 3. • Must support Bridge Extension Protocol (IEEE 802.1BR) or equivalent - to scale Gigabit & 10 Gigabit Ethernet ports • Must allow building very large L2 domain using Multi-Path Ethernet technologies. • Must support port channelling across multi chassis.
3.	Switch Features	• Must support IEEE 802.1d, IEEE 802.1w, IEEE 802.1s, IEEE 802.1q, IEEE 802.1ab, IEEE 802.3ad, IEEE 802.1p • Routing protocol support when upgraded with Layer3 License • Must support Static IP routing, OSPF, BGPv4, • Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management • Protocol Versions 2, and 3 (IGMP v2, and v3) • Support for up to 8K multicast routes • Must support In-Service Software Upgrade (ISSU) for Layer 2 • Must have Modular QoS classification compliance • It is preferred that switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center • Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)
4.	Security features	• Must support AAA using RADIUS (RFC 2138 & 2139) and/or TACACS+, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration • Must have following Access Control features • Must support Ingress ACLs (Standard & Extended or equivalent) on Ethernet and virtual Ethernet ports • Must have Egress strict-priority queuing or equivalent
5.	Quality of Service	• Must support Egress port-based scheduling: Weighted Round-Robin (WRR) or equivalent

#	Parameter	Minimum Specifications
		• Must have ACL-based QoS classification (Layers 2, 3, and 4)
6.	Compliance/ Certification	• The switch should be minimum EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program.

5.1.3.1.8 Blade Servers

#	Parameter	Minimum Specifications
1.	Processor	• Each blade shall have a minimum of two (2) latest high performance Processors with minimum 2.1GHz & 12 cores per socket. • MSI Should be go for fully populated blade configuration.
2.	Storage	Server should be configured with 2 Nos of 600 GB 12Gbps SAS 10K HDDs in Raid 0,1 .
3.	Memory	The Blade Server should be configured with minimum 128 GB of DDR4 Memory from day one.
4.	Network	• The Blade server should support Converged Network Adapter , which aggregates both the Ethernet and FC connectivity on a single controller. • The server should provide an aggregated Bandwidth of minimum 40 Gbps Ethernet & Fiber connectivity. • The server should have redundant cards to provide no single point of Failure. • In a virtualized environment, the virtualized adapter should support by passing the hypervisor. • Should be able to support VM DirectPath I/O with Vmotion on Vmware vSphere. • Adapter and QoS policies can be set and defined for each of the vNICs or vHBAs created in the virtualized adapter.
5.	Operating System	Licensed version of 64 bit latest version of Linux/Microsoft® Windows. Should support Cloud and virtualization.
6.	Management	• The Management Software should be able to manage multiple Server nodes across more than one Blade chassis and virtual machines running on these nodes. • The management software should participate in server provisioning, device discovery, inventory, configuration, diagnostics, monitoring, fault detection, auditing, and statistics collection. • The Management software should provide policy based Management using Service profiles and Templates. • It should support remote KVM capability from an external keyboard, video monitor and mouse to all blades installed in the chassis through the redundant management controllers. • Remote KVM should support up to 4 active sessions
7.	Others	Should be hot pluggable

5.1.3.1.9 Blade Chassis

#	Parameter	Minimum Specification
1.	Blade Chassis	Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit.
2.	Power	The enclosure should be populated fully with power supplies of the highest capacity & energy efficiency of a minimum of 90%
		The power subsystem should support N + N power redundancy (where N is at least equal to 2) for a fully populated chassis with all servers configured with the highest CPU configuration, maximum memory and I/O configuration possible
3.	Cooling	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics
4.	Chassis connectivity	The chassis should support redundant modules for connectivity - Ethernet and Fiber Channel /Infiniband modules OR converged fabric modules/FCoE in lieu thereof
5.	Ethernet Module	Chassis should provide minimum of 4x10G Ethernet uplinks
6.	FC Module	Chassis should host min. 4x8Gbps FC Uplinks per redundant Internal/External Switch module to connect to LAN & SAN network..
7.	Management	• Redundancy and HA should be built in the management subsystem so that if one management module/solution fails other should be able to take over automatically. Centralized Redundant Management solution should be provided so that management of all blade servers across multiple chassis within Datacenter can be done from single console. If the management system runs as a virtual machine , then all hardware and software licenses to enable this should be included
		• Role Based Access Control and remote management capabilities including remote KVM should be included
		• Movement of server identity from one slot to another in the event of server failure within chassis as well as across chassis. • Must support the ability to rollback firmware from current active versions to the previous version for the Server BIOS, Adapter firmware and bootcode versions , individual server management chips from the same console. • Role Based Access Control so that the resources can be managed by respective resource administrator. Parent administrator still have control over resources under their respective child resources • Built in high availability for the management solution and software • Embedded management within the Blade infrastructure. • Agentless internal hard disk drive monitoring and tracking • Movement of server identity from one slot to another in the event of server failure . The failover can be movement within a single chassis or across multiple chassis • Automated call home capability in the event of critical server failure or thresholds that are crossed which could impact server performance or customer SLA. • Administrators have the flexibility to define power policies so that the power can be limited to a specific server

#	Parameter	Minimum Specification
		• Administrators have the ability to set a cap on the maximum power that the chassis can draw . • Servers can be grouped and power capped for servers across multiple chassis • Integration with the Microsoft Active Directory groups • Should provide Single Pane of Glass view management for both Rack Servers and Blade Servers in a given location • Built in scheduler to set up schedules for specific actions which are disruptive . Example , set the scheduler to flash a new firmware during the weekend

5.1.3.1.10 Centralised Unified Management

#	Minimum Specifications
1	The solution shall provide a single pane of glass for automated provisioning with model-based orchestration of compute, network, storage ,applications and custom services through a unified multi-tenant IT service catalog
2	The solution shall allow authorized administrators, developers or business users to request new IT services and manage specific cloud and IT resources, while ensuring compliance with business policies
3	The solution shall support management of the machine life cycle from a user request and administrative approval through decommissioning and resource reclamation with dynamic capacity management
4	The solution shall support provisioning across multi-vendor ,multi-hypervisor (eg:VMware ESX, ESXi, Microsoft Hyper-V, and Red Hat hypervisors) physical x86, virtual and public cloud environments. Currently supported target environments with version details should be submitted as part of compliance
5	The solution shall support extensible automation and integration with northbound APIs to higher level applications.
6	The solution shall support creation of services such as 'Single VM' and a 'Multi-tier application infrastructure (including software based constructs such as load balancers)' as part of a standard template.
7	The solution shall support multiple levels of approval and email notifications with ability to automate manual provisioning and de-provisioning of the tasks and policies embedded in each layer of their application
8	The solution shall support extensibility capabilities to customize machine configurations and integrating machine provisioning /management with other enterprise-critical systems such as load balancers,network infrastructure(eg:physical, virtual switches and dynamic network topologies), configuration management databases (CMDBs), ticketing systems and IT service desk tools
9	The solution shall extend operations capabilities to the requestor of the service eg. ability to start/stop/suspend virtual machines, request additional resources and access the VM using RDP/SSH protocols through the self-service portal based on entitlement
10	The solution shall support granular role-based access control and entitlements of infrastructure services to consumers with continuous monitoring for real-time infrastructure consumption to improve capacity planning and management

11	The solution shall allow administrators to manage and reserve (allocate a share of the memory, CPU and storage) resources for a group of virtual machines to use.
12	The solution shall provide an orchestration engine with ready workflows and ability to create custom workflows based on SOAP, REST operations and PowerShell scripts
13	The solution shall integrate with Active Directory (AD) to allow importing existing users and groups in addition to creation of local users in the cloud portal.
14	The solution should support complete application lifecycle, application elements, such as middleware, databases, or web servers, must be able to configure into the infrastructure containers with integrated usage-tracking,utilization trending analysis functionality to support in built metering and chargeback

5.1.3.1.11 SAN Switch

#	Minimum Technical Specifications
1	The fibre channel switch must be rack-mountable. Thereafter, all reference to the ‘switch’ shall pertain to the ‘fibre channel switch’
2	The switch to be configured with minimum of 96 ports 16 Gbps FC configuration backward compatible to 4/8.
3	All 96 x FC ports for device connectivity should be 4/8/16 Gbps auto-sensing Fibre Channel ports.
4	The switch must have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.
5	The switch must be able to support non-disruptive software upgrade.
6	The switch must be able to support stateful process restart.
7	The switch must 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.
8	The switch must support up to 32 Virtual Fabric Instances.
9	The switch must be capable of supporting hardware-based routing between Virtual Fabric instances.
10	The switch must support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances.
11	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers.
12	The switch must support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.
13	The switch must support Smart Zoning such that the entries in the TCAM is significantly reduced and therefore increasing the overall scalability of the SAN Fabric.
14	The switch must support PowerOn Auto Provisioning (POAP) and Quick Configuration Wizard for simplified operations.
15	Inter-switch links must support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics.

#	Minimum Technical Specifications
16	The switch must support routing between Virtual Fabric instance in hardware.
17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication.
18	The switch must 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 must also be supported.
19	The switch must be equipped with congestion control mechanisms such that it is able to throttle back traffic away from a congested link.
20	The switch must be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.
21	The switch should support IPv6. It should support native switch based RESTful APIs
22	The bidder must provide atleast 2 of these switches
23	The interface requirement mentioned here is the minimum. If the solution requires more number of interfaces (considering 100% redundancy) then the same should be quoted by the bidder

5.1.3.1.12 Storage

#	Minimum Storage Requirement	TB
1.	Storage	2500

Note:

- Bidder is expected to carry out the storage requirement estimation and supply as per the solution proposed, if the estimation is more than above specified.
- Bidder may supply the storage in modular manner during the implementation

5.1.3.1.12.1 Primary Storage

#	Parameter	Minimum Specifications
1.	Solution/ Type	IP Based/iSCSI/FC/NFS/ CIFS
2.	Storage	▪ Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration) ▪ RAID solution offered must protect against double disc failure. ▪ Disks should be preferably minimum of 1.2 TB capacity for SAS and 3 TB for SATA (combination as per performance and SLA requirements of overall solution) ▪ To store all types of data (Data, Voice, Images, Video, etc.) ▪ Proposed Storage System shouldbe scalable (vertically/horizontally)
3.	Hardware Platform	Rack mounted form- factor Modular design to support controllers and disk drives expansion
4.	Controllers	▪ At least 2 Controllers in active/active mode ▪ The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
5.	RAID support	Should support various RAID Levels

#	Parameter	Minimum Specifications
6.	Cache	Minimum 64 GB of useable cache across all controllers. If cache is provided in additional hardware for the storage solution, then cache must be over and above 64 GB.
7.	Redundancy and High Availability	The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies
8.	Management software	▪ All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. ▪ Licenses for the storage management software should ▪ Include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, upto max capacity of the existing controller/units. ▪ A single command console for entire storage system. ▪ Should also include storage performance monitoring and management software ▪ Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures ▪ Should be able to take "snapshots" of the stored data to another logical drive for backup purposes
9.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours

5.1.3.1.12.2 Backup Application:

#	Description
1.	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.
2.	The solution should offer centralized, web-based administration with a single view of all back up servers
3.	The proposed backup solution should allow creating tape clone facility after the backup process.
4.	Scheduled unattended backup using policy-based management for all Server and OS platforms
5.	The proposed Backup Solution has in-built frequency and calendar based scheduling system.
6.	The software should support on-line backup and restore of various applications and Databases
7.	The backup software should be capable of having multiple back-up sessions simultaneously
8.	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
9.	The backup software 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
10.	The backup software should support different types of user interface such as GUI, Web-based interface
11.	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment.

#	Description
12.	Backup Software is able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.
13.	The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.
14.	Backup Solution shall be able to copy data across firewall.
15.	The backup software must 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 must be capable of setting this utilization threshold for tapes
16.	The backup software should be able to support versioning and should be applicable to individual backed up objects.

5.1.3.1.12.3 Tape Library

#	Minimum Technical specification
1.	Shall support Native data capacity of 100TB (uncompressed) expandable to 200TB (compressed).
2.	Shall be offered with Minimum of four LTO6 FC tape drive. Drive shall support encryption.
3.	Shall be offered with minimum of 48 Cartridge slots and scalable to minimum 100 Cartridge
4.	Tape Library shall provide 8 Gbps native FC connectivity to SAN switches.
5.	Library shall be able to back up the encrypted keys in a redundant fashion
6.	Tape Library shall provide web based remote management.
7.	The library should have cartridge I/O slots for secure & easy off-site backup storage
8.	1. Tape Library shall have GUI Panel 2. Shall be rack mountable. 3. Shall have option for redundant power supply
9.	Should support industry leading backup software
10.	40 LTO6 barcode labeled cartridges & 4 cleaning cartridges from the tape library OEM to be provided

5.1.3.1.13 Server/Network Rack Specifications

#	Parameter	Minimum Specifications
3.	Type	19” 42U racks
		mounted on the floor Floor 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 must be lockable on all sides with unique key for each rack Racks should have Rear Cable Management channels, Roof and base cable access
4.	Wire managers	Two vertical and four horizontal

#	Parameter	Minimum Specifications
5.	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
6.	Doors	The racks must 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.
7.	Fans and Fan Tray	Fan Housing Unit 4 Fan Position (Top Mounted) (HA) - Monitored - 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
8.	Metal	Aluminum extruded profile
9.	Side Panel	Detachable side panels

5.1.3.1.14 Manageable Edge Switch

#	Parameter	Minimum Specifications
1.	Ports	▪ 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports ▪ All ports can auto- negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports. ▪ Uplink ports supporting 1Gbps/10Gbps
2.	Switch type	Layer 3
3.	MAC	Support 16K MAC address.
4.	Backplane	Switching fabric capacity should support non-blocking architecture back plane for numbers (as per network configuration to meet performance requirements)
5.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8.	Protocols	▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority Queues, port mirroring, DiffServ ▪ Support based on 802.1p priority bits with at least 8 queues ▪ DHCP support & DHCP snooping/relay/optional 82/ server support ▪ Shaped Round Robin (SRR) or WRR scheduling support. ▪ Support for Strict priority queuing & Sflow ▪ Support for IPV6 ready features with dual stack, Support upto 255 VLANs and upto 4K VLAN IDs
9.	Access Control	▪ Support port security ▪ Support 802.1x (Port based network access control). ▪ Support for MAC filtering. ▪ Should support TACACS+ and RADIUS authentication

#	Parameter	Minimum Specifications
10.	VLAN	▪ Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN ▪ Dynamic Trunking protocol or equivalent
11.	Protocol and Traffic	▪ Network Time Protocol or equivalent Simple Network Time Protocol support ▪ Switch should support traffic segmentation ▪ Traffic classification should be based on user- definable application types: TOS, DSCP, Port based, TCP/UDP port number
12.	Managemen t	▪ Switch needs to have console port for management via PC ▪ Must have support SNMP v1,v2 and v3 ▪ Should support 4 groups of RMON ▪ Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

5.1.3.1.15 Online UPS

#	Parameter	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at Dc for at-least 60 min
2.	Output Wave Form	Pure Sine wave
3.	Input Power Factor at Full Load	>0.90
4.	Input	Three Phase 3 Wire for over 5 KVA
5.	Input Voltage Range	305-475VAC at Full Load
6.	Input Frequency	50Hz +/- 3 Hz
7.	Output Voltage	400V AC, Three Phase for over 5 KVA UPS
8.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9.	Inverter efficiency	>90%
10.	Over All AC-AC Efficiency	>85%
11.	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
12.	Battery Backup	60 minutes in full load at DC & Control room
13.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery

#	Parameter	Minimum Specifications
14.	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.
15.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
16.	Cabinet	Rack / Tower type
17.	Operating Temp	0 to 50 degrees centigrade
18.	Management Protocol	SNMP Support through TCP/IP

5.1.3.1.16 Fire Proof Enclosure

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart cards and similar devices and other magnetic media, paper documents, etc. the safe should have adequate fire protection.

#	Item	Minimum Specifications
1.	Capacity	300 Litres
2.	Temperature to Withstand	1000° C for at least 1 hour
3.	Internal Temperature	30° C after exposure to high temperature For 1 hour
4.	Locking	2 IO-lever high security cylindrical / Electronic lock

5.1.3.1.17 Structured Cabling

#	Parameter	Minimum Specifications
1.	Standards	ANSI TIA 568 C for all structured cabling components
2.	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards
3.	Certification	UL Listed and Verified

5.1.3.1.18 Electrical cabling

#	Parameter	Minimum Specifications
1.	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian Standard IECSs

5.1.3.1.19 DG Set

#	Parameter	Minimum Specifications
1.	General	Auto Starting DG Set Mounted on a common based frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. KVA rating as per the requirement.

#	Parameter	Minimum Specifications
2.	Capacity	250 KVA
3.	Fuel	High Speed Diesel (HSD) With 30 Ltr. Tank Capacity or better. It should be sufficient and suitable for containing fuel for 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.
4.	Power Factor	0.8
5.	Engine	Engine should support electric auto start, water cooled, multi cylinder, maximum 1500 rpm with electronic/manual governor and electrical starting arrangement complete with battery, 4 stroke multiple cylinders/single and diesel operated conforming to BS 5514/ ISO 3046/ IS 10002
6.	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.
7.	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following meters/indicators: ▪ Incoming and outgoing voltage ▪ Current in all phases ▪ Frequency ▪ KVA and power factor ▪ Time indication for hours/ minutes of operation ▪ Fuel Level in field tank, low fuel indication ▪ Emergency Stop button ▪ Auto/Manual/Test selector switch ▪ MCCB/Circuit breaker for short-circuit and overload protection ▪ Control Fuses ▪ Earth Terminal ▪ Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel
8.	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure shall be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand local climate. The enclosure shall have ventilation system, doors for easy access for maintenance, secure locking arrangement.
9.	Output Frequency	50 HZ
10.	Tolerance	+/- 5% as defined in BSS-649-1958
11.	Indicators	Over speed /under speed/High water temperature/low lube oil etc.
12.	Intake system	Naturally Aspirated
13.	Certifications	ISO 9001/9002, relevant BS and IS standard

5.1.3.2 ICT Software Components for Data Canter:

5.1.3.2.1 Enterprise Management System

To ensure that ICT systems are delivered at the performance level envisaged, it is important that an effective monitoring and management system be put in place. It is thus proposed that a proven Enterprise Management System (EMS) is proposed by the bidder for efficient management of the system, reporting, SLA monitoring and resolution of issues. Various key components of the EMS to be implemented as part of this engagement are –

1. SLA & Contract management System
2. Network Monitoring System
3. Server Monitoring System
4. Helpdesk System

The Monitoring system should be able to provide automated consolidated SLA reports for all the SLAs as mentioned in this RFP including real time status of various service levels achieved. The report to be available through a centralised web access / dash board the access for this to be given to at least 5 users of KSCL.

MSI will implement dedicated EMS solution to meet the SLA monitoring and other requirements as mentioned in the RFP. The implemented EMS solution to help KSCL in data driven decision making. The entire EMS implementation shall be certified by MSI also for its correctness, adequacy to meet RFP requirements and measurement of SLAs & KPIs etc.

5.1.3.2.1.1 SLA & Contract management System

The SLA & Contract Management solution should enable KSCL to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are –

#	**Description**
1.	It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
2.	The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components.
3.	The solution must follow governance, compliance and content validations to improve standardization of service level contracts.
4.	The solution should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
5.	The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
6.	The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Project.
7.	The solution should support requirements of the auditors requiring technical audit of the whole system.
8.	The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance.
9.	The solution should support SLA alerts escalation process.
10.	The solution should accept Data from a variety of formats; provide pre-configured connectors and adapters.
11.	Support for defining and calculating service credit and penalty based on clauses in SLAs.
12.	Reports (Indicative but not limited to) ▪ Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project ▪ Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more. ▪ Historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider’s performance ▪ Automatic Report creation, execution and Scheduling, must support variety of export formats including Spreadsheet, Word/Docs, Adobe PDF etc. ▪ Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardisation and governance of the surveillance project

#	Description
	▪ Drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project ▪ Real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.) — Resource utilisation exceeding or below customer-defined limits — Resource utilisation exceeding or below predefined threshold limits

5.1.3.2.1.2 Server Load Balancer:

Sr No		Minimum Technical Requirements
1	General Requirements	Should be high performance purpose built next generation multi-tenant hardware with multicore 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.
		Platform should have option to support 3rd party network functions from day one
		The appliance should have minimum 8 x10G SFP+ data interfaces from day one
		The appliance should support Minimum 64GB RAM and 1*SSL ASICS/FGPA/cards with network virtual function support
		Next generation multi-tenant platform must support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each network function must 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
		The device should support upto 65 Gbps of System throughput
		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
		The device should have the following features of throughput parameters
		1. Load balancer network function with minimum 15 Gbps of system throughput
		2. Should support upto 7 Million RPS per system
		3. Should support upto 35000 SSL Transactions per second
		4. Should Suppor minimum 20 Gbps of SSL Throughput
		5. Dedicated Management Interface
2	Technology	Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support
		The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc.
		Support for policy nesting at layer7 and layer4, solution should able to combine layer4 and layer7 policies to address the complex application integration.
		Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies to customize new features in addition to existing feature/functions of load balancer

Sr No		Minimum Technical Requirements
		Traffic load balancing using ePolicies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash ip and snmp
		Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc..
		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.
		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
		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..
		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.
3	Remote access	Proposed solution should support remote access which is 100% client less for web based applications
		must support for CIFS file share and provision to browse, create and delete the directories through web browser
		should maintain original server access control policies while accessing the file resources through VPN
		must support Single Sign-On (SSO) for web based applications and web based file server access
		Should have secure access solutions for mobile PDAs, Andriod smart phones, Ipad, Iphones.
		Should Support IPV6
		Proposed solution must 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.
		Should support following Authentication methods: - LDAP, Active directory, Radius, secureID, local database, and certificate based authentication and anonymous access.
		Should provide comprehensive and reliable support for high availability both at device level and Virtual function level
		Device level HA should support synchronization of network functions configuration from primary/master device to secondary/slave device
		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
		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
		ADC VF Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.
4	Management	The appliance should have SSH CLI, Direct Console, SNMP, and Single Console per Cluster with inbuilt reporting.

Sr No		Minimum Technical Requirements
		The appliance should provide detailed logs and graphs for real time and time based statistics
		Should capture, log and display traffic related data to analyze for security incidents.
		Should support XML-RPC for integration with 3rd party management and monitoring of the devices.
		The appliance should have extensive report and logging with inbuilt tcpdump like tool and log collecting functionality
		Should be able to send security incidents via syslog

5.1.3.2.1.3 Network Management System

Solution should provide fault & performance management of the server side infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, PA System, Emergency Call Boxes, Sensors, etc. Proposed Network Management shall also help monitor key KPI metrics like availability, in order to measure SLA's. Following are key functionalities that are required which will assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

#	Minimum Specification
1	The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solutions should provide centralized monitoring console displaying network topology map.
2	The system should 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.
3	The Solution should provide capability to monitor any device based on various versions of SNMP/IP.
4	The Solution should monitor bandwidth utilization.
5	The Solution must be capable of monitoring the availability, health, and performance of core networking devices including but not limited to CPU, memory, temperature.
6	The Solution should have the ability to issues pings to check on availability of ports, devices.
7	The Ping Monitoring should also support collection of packet loss, packet QOS, packet errors Latency and Jitters during ping checks.
8	The Solution should automatically collect and store historical data so users can view and understand network performance trends.
9	The solution should be capable of monitoring network delay and delay variation
10	The solution should provide the ability to visually represent LAN/WAN links with displays of related real-time performance data including utilizations.
11	Proposed solution should provide customizable reporting interface to create custom reports for collected data
12	The system must use advanced root-cause analysis techniques and policy-based condition correlation technology (at network level) for comprehensive analysis of infrastructure faults.
13	The system should be able to clearly identify configuration changes and administrators should receive an alert in such cases.
14	The solution should support multicast protocols too, if the overall project solution offered includes multicast.
15	The system shall support monitoring of Syslog or equivalent.
16	The solution should provide capability to add an IP device or IP Range or IP subnet with functionality supporting multiple SNMP strings.

#	Minimum Specification
17	Proposed solution shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.

5.1.3.2.1.4 Server Performance Monitoring

#	Description
1.	The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
2.	Proposed solution shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.
3.	The proposed tool must provide information about availability and performance for target server nodes.
4.	The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
5.	If the offered server/computing solution includes virtualisation, then the server performance monitoring solution must include virtualization monitoring capabilities.

5.1.3.2.1.5 Centralised Helpdesk

#	Description
1.	Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
2.	System should also automatically create tickets based on alarm type.
3.	The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident via web interface for issues related to the project.
4.	The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
5.	Centralized Helpdesk System should have integration with Network and Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help operators that for what particular alarms corresponding helpdesk tickets got logged.
6.	IT Asset database should be built and managed by the bidder, in order to carry out the scope of work items.
7.	Surveillance Network admin should be able to manually create tickets through Fault Management GUI.
8.	System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm.

5.1.3.2.1.6 Centralised Antivirus & Anti-Spam Solution

The following features are required for centralized anti-virus solution, to protect all computing resources (servers, desktops, other edge level devices, etc.):

#	Minimum technical specification
1.	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.)
2.	Personal Firewall: Firewall should block unwanted traffic, prevents malware from infecting endpoint systems, and makes them invisible to hackers.
3.	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

#	**Minimum technical specification**
	trustworthy applications and suspected malware used to automatically set the Program Control configuration.
4.	Heuristic virus scan: Should Scan files and identifies infections based on behavioral characteristic of viruses
5.	On-access virus scan :Should Scan files as they are opened, executed, or closed, allowing immediate detection and treatment of viruses
6.	Deep scan: Should Scan Runs a detailed scan of every file on selected scan targets
7.	Scan target drives: Should Specifies directories and file types to scan
8.	Scan exclusions: Should Specify directories and file extensions not to be scanned
9.	Treatment options: Should Enables choice of action agent should take upon detection of virus: Repair, rename, quarantine, delete
10.	Intelligent quick scan: Should Check the most common areas of the file system and registry for traces of spyware
11.	Full-system scan: Should Scans local file folders and specific file types
12.	Deep-inspection scan: Should Scan every byte of data on the computer
13.	Scan target drives: Should Specify which directories and file types to scan
14.	Scan exclusions: should Specify directories and file extensions not to be scanned
15.	Treatment options: Should Enable choice of action agents should take upon detection of virus: Automatic, notify, or confirm
16.	**Browser Security**
a.	Should Support latest versions leading web browsers i.e. IE, Mozilla, Chrome, Safari etc.
b.	Should Provide a dual browser mode that segregates corporate data from the Internet
c.	Should Allow users the freedom to surf with full protection against malicious software that is automatically downloaded and phishing attempts
d.	Should Secure through unique browser virtualization, heuristic anti-phishing and malware site detection
e.	Should Support Browser Virtualization
f.	Should Support Signature & Heuristic Phishing Protection
g.	Should Support Site Status Check
h.	Should Support Centralized Browser Security Policy Management
i.	Should Support Centralized Browser Security Event Logging & Reporting
17.	**Management Platform Support**
a.	Operating systems: Should Support Windows Server 2008, 2012, 2016
b.	Browsers: Should Support Internet latest version of leading web browsers
c.	Client Platform Support
d.	Should Windows 8, 10 (32 & 64 bit), Linux
18.	**Gateway Security**
a.	Should provide fast protection at the gateway across multiple protocols for inbound and outbound web traffic
b.	The solution should provide protection against malware threats on all Web 2.0 file transfer channels
c.	The solution should offer in built URL filtering with flexible policy controls, and in-depth reporting and alerts (the URL filtering license is required)

#	**Minimum technical specification**
d.	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
e.	The solution should have advanced application control capabilities with ability to monitor and control usage by end-users spanning multiple applications
f.	In terms of SMTP anti-pam scanning the solution should be capable of acting as mail relay or MTA by itself.
g.	Should have facility to block files based on file extensions over HTTP, FTP, SMTP, POP3 as well as IMAP
h.	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.
i.	System should classify traffic into protocols without relying on specific port numbers (for example, port 80 for HTTP)
j.	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
k.	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 Most common malware Network attacks Infection sources
l.	Reports should be available by IP address or user if active directory integration is done
19.	**Web Content Filtering**
a.	Should be an integrated solution within the firewall or a standalone hardware appliance.
b.	web content filtering solution should work independently without the need to integrate with proxy server
c.	Web based management through https and command line interface support
d.	should have facility to block URL based on categories
e.	The solution proposed should support at least 45+ million URLs categorized into 60+ default website categories across 50 different languages and 100+ protocol applications.
f.	URL Database should be updated regularly
g.	Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key logger
h.	should have configurable parameters to block/allow unrated sites
i.	should have configurable options to allow/deny access to web sites in case if the URL rating service is unavailable
j.	should have options to customize the block message information send to end users
k.	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.

#	**Minimum technical specification**
l.	Should have facility to configurable policy options to block web sites based on content
m.	The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories.
n.	Should have configurable policy options to define the URLs what needs to be blocked.
o.	should have configurable policy options to define the URL exempt list
p.	The solution should be able to block spywares/adwares etc.
q.	The solution should have options to block java applets, activeX as well as cookies
r.	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
s.	The solution should have options to block download of files over internet based on file extension (e.g. *.avi, *.mpeg, *.mp3 etc.)
20.	**URL Filtering Features**
a.	The solution should provide security related website categories to address specific security concerns include, but not limit to : a. Malicious Websites b. Key-loggers c. Phishing and Other Online Frauds d. Spyware – including drive-by spyware download and back channel communication by spyware installed on local client. e. Potentially Unwanted software f. Bot Network g. The solution proposed should have capabilities to block back channel communication from spyware / key-logger infected machines to hacker host sites h. The solution should have the ability to apply different policies to different users, different client IP address and address range and different user groups i. The solution should have the capability for Embedded URLs in selected search engines can also be filtered individually j. The solution should support Time based Quota policies for URL categories, users, IP, networks, user groups etc. k. The solution should have the ability for users to define ―Regular Expressions to precisely identify targeted URL. l. Solution should have dedicated categories for Adult material, gambling, Instant messaging, proxy avoidance, spyware ,malicious websites, Bots, phishing , key loggers m. The solution should provide capabilities to customize URL, either it is in the URL database or not, into user defined categories. n. 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 o. Ability to collect certain uncategorized or security related URLs to feedback, improve URL categorization and security effectiveness p. The solution should support display of web based block pages and the block pages should be customizable
21.	**Spam Filtering**
a.	The proposed solution should Stop spam, denial-of-service attacks, and other inbound email threats using industry-leading technologies and response

#	**Minimum technical specification**
	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.
b.	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.
c.	should be able to detect spam mails in SMTP, POP3 as well as IMAP protocols
d.	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.
e.	option should be available to manually configure multiple RBL& ORDBL servers to check for spam mail
f.	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
g.	Should have configurable parameter to enable HELO DNS lookup to check whether a mail is a spam or not.
h.	Should have configurable parameter to enable return email DNS lookup to check whether a mail is a spam or not.
i.	Should have provision to define banned key words and check against that key words to identify spam mails.
j.	Should have options to define mime headers and check against the same to identify spam mail.
k.	The solution should have Global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
l.	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:
m.	Email archiving, mail box archiving, file archiving, personal folders (.pst files) consolidation, journaling, discovering mails
n.	Integration with data loss prevention technologies to check loss of data through mails at gateway
o.	The proposed solution should have an option to restore an appliance to its original image configuration.
p.	Should have configurable spam actions for detected spam mails (e.g. tag the mail, delete the spam mail etc.).

5.1.3.2.1.7 Mailing and Messaging Solution

#	**Minimum technical specification**
1.	**General**
a.	Network/Server edition should run on Linux /Windows.
b.	Desktop client should run on Mac, Linux and Windows.

c.	Solution should be based on open standards
d.	Should support advanced search and file indexing for large inboxes
e.	Ability to use custom logos in the web interface
f.	Should support e-mail, Address Book, Calendar, Task & File Server
g.	Should support real-time backup and restore
h.	Should support clustering/High-Availability
i.	Ability to access the Mail server via IMAP clients, with the option to connect over SSL/TLS
j.	Ability to access the Mail server via POP clients, with the option to connect via SSL/TLS
k.	Comprehensive suite of standards-based web services APIs enabling seamless integration with other applications
l.	Ability to utilize Active Directory for user authentication and/or Global Address List
m.	Admin can configure an initial password in the migration wizard and import wizard for newly provisioned accounts
n.	Should support multi-tenancy
o.	Should support e-mail Archiving & Discovery
p.	Should have rich, interactive, web-based interface for end user functions (access via HTTP or HTTPS)
q.	Ability to customize the colors and appearance of the web interface
r.	Option to check and correct spelling in a mail message, calendar appointment, or web Document
s.	Ability to share Address Books, Calendars, and Notebooks (Documents) with internal users and groups (read or write access)
t.	Ability to share Address Books, Calendars, and Notebooks (Documents) with external users via a custom password (read access)
u.	Ability to quickly categorize messages, contacts, and/or documents by attaching "Tags" with user-defined names and colors
v.	Option to quickly view attachments in HTML format
w.	Should support conversations span folders
x.	Ability to create personal folders and folder hierarchies
y.	Ability to print a message and see a print preview
z.	Ability to sort messages based on subject, date, or sender
aa.	Ability to flag/unflag messages/conversations for follow up
bb.	Ability to define filter rules and priorities for incoming messages
cc.	Ability to enable/disable a custom away message
dd.	Ability to add a custom signature to a message
ee.	Option to popup a separate window when composing a message
ff.	Ability to save in-progress messages to a Drafts folder
gg.	Ability for a user to set an automatic forwarding address and choose whether to leave a copy in the primary mailbox
hh.	Option to Reply or Reply-All while retaining the attachments from the original message
ii.	Right-clicking a message displays a menu of actions to take on that message (e.g. Mark Read, Reply, Delete)
jj.	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)
kk.	Ability to export a set of messages as a ZIP file
ll.	Ability to toggle between Reply and Reply-All while composing a reply
mm.	Users can set their default preference for viewing messages in the reading pane

nn.	Users can set the default font family, font size and font color to use when composing email messages and Documents pages
oo.	Users can share their mailbox folders and set the permission levels to manage or to view-only.
pp.	Users can insert inline images in email messages and calendar appointments
qq.	Admins can configure the maximum number of characters used in a signature
rr.	Admin can define expiration policy for individual mailbox folders
ss.	Users will receive an email message warning of quota usage based on a threshold defined by administrator
tt.	Users can attach a URL to an email message
uu.	Users can double-click on a message in message view to expand the view pane to full view
vv.	Users can define multiple email signatures to use
ww.	Users can check multiple emails in the list view to mark as read/unread/tag, delete, or to move to a different folder
xx.	When sending a message, the priority is normal, but it can be set to high or low as well
yy.	Users can get immediate notification of new mail
zz.	Multiple messages can be selected and forwarded in one email
aaa.	Users can right click on a folder to see the number of messages and the total size of items in folder
2.	**Address Book**
a.	Business card view of Contacts
b.	List view of Contacts with preview pane
c.	Ability to import/export Contacts in .csv format
d.	Ability to import/export contacts in vCard (.vcf) format
e.	Ability to print a single Contact or list of Contacts and see a print preview
f.	Right-clicking a Contact displays a menu of actions to take on the Contact (e.g. compose message, search for messages)
g.	Ability to drag a Contact to a mini-calendar date to create an appointment with that Contact
h.	Ability to create multiple Address Books in a single mailbox
i.	Ability to move/copy contacts from one Address Book to another (based on access privileges)
j.	Ability to create group contact lists in their user Address Books
k.	Address book displays individual contact information in tabbed view
l.	Photos and images can be uploaded to contacts in Address Books
3.	**Calendar**
a.	Ability to schedule personal appointments
b.	Ability to schedule meetings and view attendees' free/busy information
c.	Ability to create recurring meetings and exceptions to recurring meetings
d.	Ability to book resources (locations, equipment, etc.) for a meeting
e.	Ability to configure a resource to auto-respond to scheduling requests based on availability
f.	Option to enable an alert popup for upcoming appointments
g.	Appointments/schedules are automatically displayed in the users current time zone
h.	Ability to set an explicit time zone for an appointment
i.	Ability to view calendars in Day, Week, Work Week, or Month views

j.	User setting for the first day of the week; value chosen impacts the Week calendar view
k.	Ability to create an appointment and/or drag an appointment's boundaries inline in calendar views
l.	Ability to quickly mark Accept/Tentative/Decline from calendar views
m.	Declined appointments display faded so that the user remains aware of their occurrence
n.	Ability to print calendars in day, week, work week, or month views and see a print preview
o.	Hovering over an appointment in calendar view displays additional appointment details
p.	Option to display a miniature calendar at all times
q.	Hovering over a date in the mini-cal displays calendar information for that date
r.	Right-clicking on the mini-cal displays a menu of actions to take on the associated date (e.g. add appointment, search for messages)
s.	Ability for a user to create multiple calendars within a single account
t.	Ability for a user to designate which calendars will be included in the user's free/busy calculations
u.	Ability to subscribe to an external calendar in iCalendar (.ics) format
v.	Ability to publish/export a calendar in iCalendar (.ics) format
w.	Ability for a user to view multiple calendars overlaid in the same view, which each calendar optionally represented by a different color
x.	When viewing multiple calendars, option to view that indicates the degree of conflict at each potential time slot
y.	Users can import calendar iCalendars (.ics)
z.	Appointments can be marked as private or public.
aa.	Administrators can configure the Calendar feature to be able to create only personal appointments
bb.	Users can search for appointments within their calendars
cc.	Public calendars display in HTML read-only format
4.	**Tasks**
a.	Add tasks and set the start and due date, set the priority and keep track of the progress and percentage complete
b.	Share task lists with internal and external users and set permission levels to manage or to view-only
c.	Users can organize task lists into folders
d.	Users can sort tasks by Status or Due Date
e.	Users can set the priority of tasks to high, normal or low
f.	Individual tasks can be tagged
g.	Files can be attached to a tasks
5.	**Documents**
a.	Ability to create rich web Documents with WYSIWYG or HTML editing
b.	Ability to create a notebooks as a Document repository and as a mechanism for navigating through Documents
c.	Ability to create multiple notebooks in a single mailbox
d.	Ability to create a notebook that is shared by everyone within a domain
e.	Ability to insert links in Documents to other Documents or to external URLs
f.	Ability to upload Attachments as Documents
g.	Ability to embed rich content objects as independently editable items inside a web Document

h.	Ability to embed an image as an ALE object inside a web Document
i.	Ability to embed a spreadsheet as an ALE object inside a web Document
j.	Ability to print a Document and see a print preview
k.	Pages show when last modified and version
l.	Users can upload files to their mailbox and can access them from any computer
m.	Users can add email attachments to a selected folder
6.	**Search**
a.	Server-side indexing of mailbox content, enabling fast and efficient search from g g g the web interface
b.	Ability for a search to include any number of conditions combined via Boolean-like expressions (AND, OR, NOT, etc.)
c.	Ability to use text commands to execute searches
d.	Advanced interface for building searches
e.	Ability to search for a specific item type (Mail, Contacts, Documents, etc.) or across item types
f.	Ability to search using a prefix plus a wildcard
g.	When using Search Builder, the search result set updates continuously as search conditions are changed
h.	Ability to save searches for subsequent one-click re-execution
i.	Ability to search for items that contain specific keywords
j.	Ability to search for items with a specific date or within a specific date range
k.	Ability to search for items that contain an attachment
l.	Ability to search for items that contain an attachment of a certain type(s)
m.	Ability to search for items that have a specific flagged/unflagged status
n.	Ability to search for items that are in a specific folder
o.	Ability to search for items based on storage size
p.	Ability to search for items based on read/unread status
q.	Ability to search for items with specific recipients in the To /Cc fields
r.	Ability to search for items from a specific sender
s.	Ability to search for items based on subject
t.	Ability to search for items that include a specific Tag(s)
u.	Ability to search for items that were sent to or received from a specific domain
v.	Ability to search for Contacts in a Shared Address Book
w.	Ability to search for content inside attachments
x.	Can search for appointments in calendars up (up to 180 days)
y.	Administrator can disable the indexing of junk mail
7.	**Domain-Level Management**
a.	Ability to create and manage multiple mail domains within a single instance of Messaging Solution
b.	Ability to use different Global Address Lists for each domain
c.	Ability to use different authentication stores for each domain
d.	Ability to delegated domain-level administrators to manage users and other settings specific to a domain
e.	Ability to create domain-specific custom branding of the web interface
f.	Ability to enable a domain admin to update account quotas up to a maximum set value
g.	Ability to set quota for each domain (either unlimited or a maximum value per account)
h.	Ability to move a domain

i.	Ability to search across mailboxes from the administration console
8.	**Storage**
a.	Messages (including attachments) sent to multiple users are stored once to optimize storage space
b.	Ability to set quotas for mailbox size and number of Contacts
c.	View of mailboxes sortable by quota, total mailbox size, or % quota consumed
d.	Ability to define retention policies for all messages, trashed messages, and/or junk messages
e.	Ability to move a mailbox(es) from one server to another without requiring system downtime or affecting other mailboxes
f.	Ability to run a regularly scheduled process that moves older messages to a secondary storage volume
9.	**System Health & Security**
a.	Should have native anti-virus & anti-spam mechanism
b.	Administrator interface setting to specify spam quarantine and kill thresholds
c.	Messages that users mark as Junk / Not Junk are automatically fed into the spam training engine
d.	Administrator interface setting to define the update frequency for virus signatures
e.	Ability to enforce client authentication to the SMTP server before relaying mail (with option to require authentication over TLS)
f.	Graphical display of system activity including disk usage, message volume, and AS/AV results
g.	Ability to monitor the status of all core system servers/services in a single view
h.	Ability to block attachments based on criteria such as attachment type or size
i.	Ability to enforce that attachments be viewed as HTML, enabling risk-free attachment viewing without requiring attachment-native applications on the viewer's machine
j.	Install and manage certificates from the administration console
10.	**Compatibility & Interoperability**
a.	MAPI-based synchronization of mail, contacts, and calendar data between Outlook and the proposed solution server
b.	Online/offline status is automatically detected, enabling the user to work without having to specify their connection status
c.	Synchronization operations are cached and synchronized as an asynchronous process, enabling optimal Outlook performance
11.	**Mobile Devices**
a.	AJAX Mobile Web Browser
b.	iPhone Email, Contact, Calendar sync
c.	Windows Mobile and other smartphone Email
d.	Email, Contact, Calendar sync

5.1.3.2.1.8 Identity Access Management

SL. No.	**Description**
1	**Identity Management**
3.1	The Identity and access management should be able to provide complete user lifecycle identity management for all types of users.
3.2	The solution should provide identity management, governance and Identity management portal, including entitlement certification and role management

SL. No.	Description
3.3	The proposed solution should provide user provisioning and de-provisioning on all target systems, automatic account provisioning, removal, and approval processes throughout the user's entire lifecycle.
3.4	The proposed solution should have customizable workflows to support the unique way environment approves, alerts, and schedules these activities.
3.5	The proposed solution should provide centralized control of identities, users, roles and policies across on-premise and cloud applications.
3.6	The proposed solution should provide User self-service to manage attributes of their own identities, reset passwords and request access to resources.
3.7	The proposed solution should support Password Synchronization to reflect changes in identity management systems and target applications
3.8	The proposed solution provide Privilege cleanup by examining existing system entitlements and highlights excessive or unnecessary privileges. Delivers details such as such as how often a resource was accessed or if an entitlement causes a security policy violation.
3.9	The proposed solution should provide Identity and access governance policies using centralized engine that helps establish and enforce a consistent set of business and regulatory compliance policies.
3.10	The proposed solution should support Entitlements certification by providing easy to use interface through which managers or resource owners can view and certify that privileges are appropriate or should be removed, thus helping meet compliance requirements.
3.11	The proposed solution should support Role modelling analysis to efficiently sort through extremely large volumes of user and privilege information to discover potential roles.
3.12	The system should be able to detect any changes in the target systems via the concept of reverse synchronization and associate various actions upon detection
3.13	The solution should have ability perform bulk jobs for example user changes, scheduled jobs
3.14	The proposed solution should offer an easy-to-use, configurable user-centric Risk Model that identifies areas of risk caused by users with high risk scores.
2	**Single Sign on under Identity Management**
4.1	The solution should have a capability which helps to prevent unauthorized users from hijacking legitimate sessions with stolen cookies and assures that the client who initiated the session is the same client that is requesting access.
4.2	The solution should have capability to support various SSO architectures that can be used independently or mixed and match to meet various business needs such as: — Agent-based policy enforcement points — Centralized gateway enforcement points — Support for today's open standards including SAML, OAuth, OpenID and WS-Federation — Agent-less based approach to securely pass claims to applications without the use of proprietary APIs — REST and SOAP-based Web APIs to allow applications to remotely call Single Sign-On as a Web service for authentication or authorization

SL. No.	Description
4.3	The solution should provide secure single sign-on and flexible web access management to applications and Web services either on-premise, in the cloud, from a mobile device or at a partner's site.
4.4	The solution shall support SSO by passing the user's identity among heterogeneous servers securely. No additional authentication is required.
4.5	The solution should provide session assurance.
4.6	The solution should provide centralized session management to securely manage a user's online session.
5	**Privilege Access Management Under Identity Management**
5.1	The proposed solution should be appliance based and provide the capability to manage Password Vault, Access Management, Session Recording, Application to Application (allows dynamic password access from applications), etc. within a single hardened platform.
5.2	The proposed solution should supports a process to automatically synchronize with a DR site over a WAN and provide built-in replication of the password vault aiding disaster recovery
5.3	The Proposed solution should have ability to define a zero trust, explicitly allow only access methodology.
5.4	The proposed solution should provide built in Active-Active High Availability and Load Balancing along with built-in clustering without the use of a traffic load balancer.
5.5	The Proposed solution should have ability to provide real-time data synchronization among a cluster.
5.6	The proposed solution should not require using third party software or hardware such as Operating Systems, Databases, High Availability, Load Balancers, etc.
5.7	The proposed solution should be browser independent and there shouldn't be any browser dependency to manage and record the sessions.
5.8	The proposed solution should provide highly efficient integrated video session recording with low storage requirements.
5.9	The proposed solution should provides in-line command filtering using white lists/black lists for SSH, network devices command line operations.
5.10	The proposed solution should be able to support application based session via RDP protocol in which the user can be confined, rather than requiring RDP to a full desktop.
5.11	The proposed solution should support to require an approval by designated users as a condition of accessing the credentials for managed accounts. The Solution should also enforce users to specify reason when requesting access for a privileged account.
5.12	The proposed solution should provide tools/APIs for enabling applications that require access to privileged accounts to access credentials programmatically, eliminating the need to "hard code" credentials into the script or application. Password should be rotated automatically.
5.13	The Proposed solution should have ability to manage target OS, Databases, Network, security devices, Virtual and cloud environments local administrator credentials through single appliance.
5.14	The proposed solution should provide threat analytics that provides a continuous, intelligent monitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage.
6	**Host Based Access Control Under Identity Management**

SL. No.	Description
6.1	The proposed solution should provide granular access control on critical Servers to protect the access even if the servers are accessed directly from the console.
6.2	The proposed solution should support all Unix, Linux and Windows platforms and should be agent based.
6.3	The proposed solution should control and monitor privileged user access to files, folders, processes and registries, enabling accountability, incoming/outgoing TCP/IP protection, integrity monitoring and segregation of duties.
6.4	The proposed solution should restrict superuser privileges with finer level of granularity than what is available in the host operating system.
6.5	The proposed solution should support authentication to Linux and Unix using Windows AD credential and also provide User ID management (including UNIX files and NIS)
7	**Authentication under Identity Management**
7.1	The proposed solution should provide PKI and Risk Based authentication. It should also support mobile OTP.
7.2	The proposed solution should have tight integration with proposed SSO solution
7.3	The proposed solution should have Pre-built rules that cover typical fraud patterns.
7.4	The proposed solution should support customization of pre-built rules or creation of new rules quickly and easily.
7.5	The proposed solution should Self-learning scoring engine based on statistical modeling
7.6	The proposed solution should have Device identification mechanism using multiple variable device fingerprinting
7.7	The risk based engine should also use geo location criteria
7.8	The proposed solution should have policy-based system to flag and manage cases of suspicious activity.
7.9	The proposed solution should Integrate data from multiple channels.
7.10	The proposed solution should learn end user behavior and suggests step-up authentication when there is a deviation from normal behavior.
7.11	The proposed solution should support out of band authentication via SMS, Email and Voice including mobile push.

5.1.3.2.1.9 Enterprise Database

#	Description
1.	Database License should be un-restricted and perpetual, to prevent any noncompliance in an event of customization & integration.
2.	Databases shall support multi-hardware platform.
3.	RDBMS should support Unicode with Indian Language support
4.	RDBMS should have spatial capability and should be capable of storing vector (2D, 3D), raster data as well as the metadata.
5.	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.
6.	Database shall have built-in backup and recovery tool, which can support the online backup.
7.	RDBMS should support of seamless data transformation from on premise to public cloud and from public cloud to on premise.
8.	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically

#	Description
	balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.
9.	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single /multiple database.
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.
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
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.
13.	Ability to recover the node on fly or with limited timelines with-out Unloading/ reloading data.
14.	RDBMS should provide continuous availability features to address hardware failures, instance failures, human errors like accidental deletion of data, tables etc.
15.	Database shall provide native functionality to store and retrieve XML, Images and Text data types.
16.	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
17.	RDBMS should support spatial data types.
18.	Database shall have Active-Passive or Active-Active failover clustering with objectives of scalability and high availability.
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 database.
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.
21.	Database shall be having native auditing capabilities for the database.
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.
23.	Availability of recovery/restart facilities of the DBMS.
24.	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
25.	Program restart should be provided from the point of failure.
26.	RDMS should have the ability to manage recovery/restart facilities to reduce system overhead.
27.	Provides extra utilities to back up the databases by faster means than record by record retrieval.
28.	The database should provide controls over who, when, where and how applications, data and databases can be accessed.
29.	RDBMS should be possible to prevent privileged IT users such as DBAs and administrators from accessing and modifying the data.
30.	The database should provide multi-factor authentication based controls and policies preferably taking account of application context etc.
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.
32.	System should record the date and time stamp for all records generation/modification.
33.	Solution should offer spatial analytic functions for data mining applications, such as binning, spatial correlation, co-location mining, spatial clustering, and location prospecting

5.1.3.2.1.10 Enterprise Backup Software

#	Description
17.	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.
18.	The solution should offer centralized, web-based administration with a single view of all back up servers
19.	The proposed backup solution should allow creating tape clone facility after the backup process.
20.	Scheduled unattended backup using policy-based management for all Server and OS platforms
21.	The proposed Backup Solution has in-built frequency and calendar based scheduling system.
22.	The software should support on-line backup and restore of various applications and Databases
23.	The backup software should be capable of having multiple back-up sessions simultaneously
24.	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
25.	The backup software 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
26.	The backup software should support different types of user interface such as GUI, Web- based interface
27.	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment.
28.	Backup Software is able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.
29.	The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.
30.	Backup Solution shall be able to copy data across firewall.
31.	The backup software must 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 must be capable of setting this utilization threshold for tapes
32.	The backup software should be able to support versioning and should be applicable to individual backed up objects.

5.1.3.2.1.11 Directory Services

#	Description
1.	Should be compliant with LDAP v3
2.	Support for integrated LDAP compliant directory services to record information for users and system resources
3.	Should provide authentication mechanism across different client devices / PCs
4.	Should provide support for Group policies and software restriction policies
5.	Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
6.	Should provide support for X.500 naming standards

#	Description
7.	Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
8.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
9.	Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
10.	Should support directory services integrated DNS zones for ease of management and administration /replication.

5.1.3.3 Disaster Recovery and DR Cloud

a) MSI shall also be responsible for providing Cloud service for storing all applications at DR [minimum 50% production capacity, RTO – 60 mins, RPO – 15 mins] which will be implemented under Kanpur Smart City project for the project duration.

b) All applications need to have high performance clustering (redundancy) within the Data Centre with heartbeat, automatic fail-over, and redundant data storage is 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 must be active-active configurations. Active passive configurations may be permissible for supporting applications.

c) The proposed Cloud Service Provider (CSP) must be an empaneled cloud service provider by Meity (Ministry of Electronics and Information Technology for Public cloud, Virtual Private Cloud and Community Government Cloud.

d) The Cloud Data Centre Facility must be within India and must be Tier III or above. The DR site within India should be at least 250 Km away from the KSCL Data Center and in a different seismic zone.

e) The Cloud Data Centre, where cloud hosting is proposed, must have ISO 27001 certification.

f) The cloud service provider must have billing model of pay-per-consume where it will charge for amount of computing resources being consumed by application rather than for the allocated resources. MSI shall provide the rate chart of the cloud services to KSCL.

g) Cloud services should be accessible via Internet, Point to Point / MPLS, Leased Lines, OFC WAN etc. MSI must provide private connectivity between KSCL's network and Cloud Data Centre Facilities.

h) 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.

i) MSI shall provide interoperability support with regards to available APIs, data portability etc. for KSCL to utilize in case of Change of cloud service provider, migration back to Local Data Centre, burst to a different cloud service provider for a short duration or availing backup services from an alternate Cloud service provider.

j) 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.

k) KSCL shall retain ownership of all virtual machines, templates, clones, and scripts/applications created for KSCL's applications. KSCL shall retain the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

l) 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.

m) Additional Parameters

- Cloud services should be accessible via internet and MPLS.

- MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications
- 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.
- MSI should offer dashboard to provide visibility into service via dashboard.
- MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the approval of the KSCL.

The below High Level Design (HLD) is just for reference over cloud deployment. MSI can suggest security stack & deployment method according to their recommendations;

5.1.3.3.1 Preparation of Disaster Recovery Operational Plan

The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with KSCL 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

MSI shall provide DR Management (DRM) Solution to KSCL meeting following specifications:

#	Features
1	The proposed solution must 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
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	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

5.1.3.3.2 Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

- Devising and documenting the DR policy discussed and approved by KSCL.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit

5.1.4 Network Backbone and Internet Connectivity

5.1.4.1.1 Overview

Pan city network backbone and internet connectivity is an important components of the project and needs very careful attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance. City wide network is essentially intended to provide a high-speed network connectivity for supporting all existing and future smart solutions. The project objectives broadly are as follows:

- 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

The proposed smart city solution will involve city wide network coverage across various locations in KSCL. Kanpur smart city will offer various smart services to its citizens. To provide these services in an uninterrupted and effective manner a robust network is required to be deployed. Network needs to be planned to meet the all the network requirements for currently services envisaged, scalability and future requirement. KSCL intends to provide connectivity under at locations like; municipal offices, BRT depots, traffic junctions, parks, fire establishments, police stations, urban health centers, schools etc. MSI would be required to create a single network i.e. city wide network for the smooth functioning of all solutions. Successful bidder is required to integrate city wide network with Data center (DC), Disaster recovery (DR) and Command Control & Communication Center (ICCC).

KSCL intends to procure Leased Circuits & Internet Bandwidth for the city wide network under the Kanpur smart city Project. The successful bidder is required to terminate the desired Leased circuits and Internet Bandwidth at the locations specified.

A Service Level Agreement will be signed with the successful bidder. As bidder, will be responsible for smooth functioning of the entire network connectivity, availability of sufficient quantities of all the critical components will be taken care of by the bidder to maintain the guaranteed uptime. Bidders are requested to take into consideration the equipment’s required at each location for providing connectivity while quoting for the tender.

Full Duplex Bandwidth as Per Schedule of Requirement has to be provisioned and implemented by the Service Provider. Service Provider has to keep provision of giving burstable Bandwidth & the rates will be as per finalized rates. Service Provider has to arrange fiber & other last mile equipment accordingly including media convertors wherever required.

5.1.4.1.2 Scope of work

The detailed scope of work for MSI for providing of pan city network backbone is given below:

5.1.4.1.2.1 Bandwidth Provisioning

MSI shall implement the solution in and provision the network bandwidth as per details given below. MSI shall be responsible for upgrading its infrastructure, including the last mile, to meet the requirements of the KSCL, at no additional cost to the KSCL. The network & bandwidth should meet following requirements:

- KSCL may order an increase/decrease/termination/withdrawal in bandwidth, which bidder 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.

5.1.4.1.2.2 Internet Bandwidth at ICCC, Data Center and all field locations

- KSCL is procuring bulk internet bandwidth for the requirement of various locations throughout the city. MSI is required to terminate these links at the desired locations defined as per the price bid format of this RFP.

5.1.4.1.2.3 Redundancy

- As a measure of redundancy remote locations, ICCC, DC & between DC & DR site connected through Leased Circuits should have redundancy in place to meet necessary SLA requirements.
- Location-wise Bandwidth requirements is given in Annexure A & B.

5.1.4.1.2.4 Rate Contract

- KSCL is procuring leased circuits to be delivered at various locations spread across the Kanpur city.
- Looking at the scalability and future requirement discovery of prices shall be valid for the period contract duration under the Rate Contract as per price bid.
- It has been observed that there is a considerable price reduction in cost of Domestic and Internet bandwidth during last few years. Hence, KSCL will review the prices at end of every year and MSI is required to match the prevailing market prices as per TRAI regulations.
- Adding new location – whenever a new location is decided to be added by the KSCL, 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.

5.1.4.1.2.5 Technical Specifications

a. Leased circuit:
   - The bandwidth must be provisioned on Optical Fiber Media. No other last mile media type is acceptable.
   - Latency from point A to point B should not exceed 20 ms.
   - The bandwidth supplied should be symmetric, dedicated 1:1 with 100% throughput.
   - Up time guarantee must be 99.5 %
   - MSI must deliver this bandwidth on a fiber optic cable network at the respective locations.
   - All costs to connect the links to last mile node of SCADL has to be borne by MSI. KSCL will not pay or reimburse any last mile of extra work cost.
   - MSI has to use the IP addressing schema provided by the SCADL.

b. Internet Bandwidth
   - The bandwidth must be provisioned on Optic Fiber media only. No other last mile media type is acceptable.
   - KSCL is procuring bulk internet bandwidth (as per the Price bid) for the requirement of various locations throughout the city. However, successful MSI is required to terminate these links at the desired locations.
   - Latency to Google, Yahoo and NIXI peering should not exceed 200 ms.
   - The bandwidth should be dedicated 1:1 with 100% throughput.
   - Up time guarantee must be 99.7%
   - Provider must have minimum two sources of Internet Gateway bandwidth input.
   - MSI must deliver this bandwidth on Gigabit Ethernet optically or electrically which will be taken as input.

- MSI must deliver the required bandwidth on a fiber optic cable network at the desired locations.
- All costs to connect the link to the last mile node has to be borne by MSI. KSCL will not pay or reimburse any last mile of extra work cost.

5.1.5 Smart Urban Solution

MSI has to implement below mentioned solutions as per city requirement where provision of Artificial Intelligence plays key important role. Various uses case are required to configure in integrated way at edge and at backend of ICCC. Following minimum use cases to be comply and implement using Edge analytics by the CCTV cameras and continuous learning capability through Artificial Intelligence :

- Graffiti and Vandalism detection
- 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
- 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
- Safety: Detection and classification based on :
    - 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

Above use cases but not limited to has to be implement by MSI as part of overall solution for various smart solution service delivery to citizens and city governance

5.1.5.1 Integrated Traffic Management System (ITMS)

5.1.5.1.1 Overview:

Adaptive Traffic Control System (ATCS): ATCS have following major Components

- Traffic Signal Controller
- Countdown timer
- Communication Network
- Software Application

<u>Traffic Signal Controller</u>

1.The Traffic Signal Controller equipment is a 32 bit or 64 bit microcontroller with solid state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during manual override phase.

2.The Traffic Signal Controller will be adaptive so that it can be controlled through the central traffic control Centre as an individual junction or as part of group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through central command controller easily

3.Site specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction specific plans or signal timings.

4.All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.

5.The controller shall provide a real time clock (RTC) with battery backup that set and update the time, date and day of the week from the GPS. The RTC shall have minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day.

6.The controller shall have the facility to update the RTC time from ATCS server, GPS and through manual entry.

7.The traffic signal system including controller shall have provision audio output tones and should be disabled friendly for.

8.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.

Traffic Signal Controller Operating Parameters

- Phases - The controller shall have facility to configure 32 Phases either for vehicular movement, filter green, indicative green, pedestrian movement or a combination thereof.
- 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.
- The pedestrian phase signal shall be configured for flashing red or flashing green aspect during pedestrian clearance.
- It shall be possible to configure any phase to the given lamp numbers at the site.
- Stages – The controller shall have facility to configure 32 Stages
- Cycle Plans – The controller shall have facility to configure 24 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.
- 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.
- Special Day Plans – The controller shall have facility to configure a minimum of 20 days as special days in a calendar year.
- 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.
- 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.
- 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 preempt the Minimum Green once the stage start commencing execution.

- 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.
- Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status
- 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.
- 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.
- Fixed Time mode with fixed offsets
- Vehicle Actuated mode with fixed offsets

Input and Output facilities

1.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

2.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.

3.Communication Interface: The traffic signal controller shall support Ethernet interface to communicate with the ATCS server

4. 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.

5. 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.

6. The traffic signal controller shall update the date, time and day of the week automatically from GPS during power ON and at scheduled intervals.

7.Manual entry for date, time and day of week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).

8.It shall be possible to set the RTC from the Central Server when networked

9.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

10.Operator Display (optional): The traffic signal controller shall optionally have a LED backlit Liquid Crystal Display (LCD) as the operator interface.

Countdown Timer:

It shall be installed at each traffic junction under ITMS & City Surveillance System Project.

- Count Down Timer to be configured in Vehicular Mode.
- The Vehicular countdown timer should be dual
- color,; Red for Stop or STP and Green color for Go
- There should be alternate Red and Balance phase time for STOP or STP in Flashing

- Alternate Green and Balance Phase Time for Go in Flashing

Communication Network : Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the Central Computer in ICCC. Central Computer running the ATCS application shall calculate and send optimum signal timings to all intersections in the corridor. MSI shall clearly specify the bandwidth requirements and the type of network recommended for the ATCS.

The contractor shall specify the networking hardware requirements at the ICCC and remote intersections for establishing the communication network.

ATCS Software Application

Objective of the ATCS is to minimize the stops and delays in a road network to decrease the travel time with the help of state-of-the-art technology. The adaptive traffic control system 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 signal controllers connected to it. These calculations will be based up on assessments carried out by the ATCS application software running on a Central Computer based on the data and information gathered by vehicle detectors at strategic locations at the intersections controlled by the system.

The ATCS application software shall do the following:

#	Description
1.	Identify the critical junction of a corridor or a region based on maximum traffic demand and saturation.
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.
3.	Stage optimization to the best level of service shall be carried out based on the traffic demand.
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.
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.
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.
7.	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real time demand
8.	Propose timing plans to every intersection under the ATCS in every Cycle
9.	Verify the effectiveness of the proposed timing plans in every cycle
10.	Identify Priority routes
11.	Synchronize traffic in the Priority routes
12.	Manage and maintain communication with traffic signal controllers under ATCS
13.	Maintain database for time plan execution and system performance
14.	Maintain error logs and system logs
15.	Generate Reports on request

#	**Description**
16.	Graphically present signal plan execution and traffic flow at the intersection on desktop
17.	Graphically present time-space diagram for selected corridors on desktop
18.	Graphically present network status on Desktop
19.	Make available the network status and report viewing on Web
20.	The ATCS shall generate standard and custom reports for planning and analysis
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
22.	Shall have the 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.
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 liked with real time traffic data fusion and control of traffic signaling infrastructure on ground.
24.	Shall collect continuously information about current observed traffic conditions from a variety of data sources and of different kind (traffic states, signal states, vehicle trajectories, incidents, road works, etc.).
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).
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.
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.
28.	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results
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
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)
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”
32.	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.
33.	Shall operate in real time that is continuously updating the estimates on the state of the network and the travel times on the basis of data collected continuously over time.
34.	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the continuously throughout the network
35.	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller
36.	Reports: a. Intersection based reports • 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 preemption time).

#	Description
	• 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. • 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. • 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. • Mode switching report – The report shall give details of the mode switching taken place on a day. • Event Report - The report shall show events generated by the controller with date and time of event. • Power on & down: The report shall show time when the master is switched on, and last working time of the master controller. • 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 LDR with time stamp. • Plan Change – The report shall show the time of change of plan either through keypad or remotely through a PC or Server. • RTC Failure – The report shall show the time when RTC battery level goes below the threshold value. • 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. • 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. • Lamp Status Report – The report shall show lamp failure report with date and time of failure, colour of the lamp and associated phase. • Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase. • Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with other phase. b. 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 c. 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.
37.	Graphical User Interface - The application software shall have the following Graphical User Interface (GUI) for user friendliness. • User login – Operator authentication shall be verified at this screen with login name and password • 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. • 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. • Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.

#	Description
	• Reports Printing / Viewing – This link shall allow selection, viewing and printing of • different reports available under ATCS • Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history. • Junctions shall be plotted proportional to their distance on Y-axis and time elapsed for the stage in seconds on X-axis. • Junction names shall be identified with each plot. • Facility shall be available to plot the time-space diagram from history. • Currently running stage and completed stages shall be identified with different colours. • Stages identified for synchronization shall be shown in a different colour. • Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions. • It should be possible to freeze and resume online plotting of Time-Space diagram. • The system shall have other graphical interfaces for configuring the ATCS, as appropriate.

5.1.5.1.2 Scope of Work

5.1.5.1.2.1 Automatic Number Plate Recognition (ANPR) System

5.1.5.1.2.1.1 Overview

ANPR System shall enable monitoring of vehicle flow at strategic locations. The system shall support real-time detection of vehicles at the deployed locations, recording each vehicle, reading its number plate, database lookup from central server and triggering of alarms/alerts based on the vehicle status and category as specified by the database. The system usage shall be privilege driven using password authentication. System should have following functional requirements:

5.1.5.1.2.1.2 Scope of Work

System should have following components and capable of doing following:

- Ability to have IR illuminators to provide illumination for night-time scenario.
- Ability to provide the live feed of the camera at the integrated command control and center or as per user requirement.
- Ability to provide video clips of the transaction from the ANPR lane cameras as evidence.
- Ability to detect the color of all vehicles in the camera view during daytime. The system can store the color information of each vehicle along with the license plate information for each transaction in the database.
- Ability to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations
- Ability to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc. by authorized personnel.
- Ability to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories.
- Ability to generate automatic alarm to alert the control room on successful recognition of the number plate based on pre-defined rules.
- Ability to easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.
- Ability to generate MIS reports to concerned authorities and facilitate optimum utilization of resources. These reports shall include but not limited to:

  - Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.
  - Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.
  - Report of Vehicle Status change in different Vehicle Categories.
- Ability to search the information based on parameters defined.
- Ability to auto generate reports and send to stakeholders.
- Ability to define system access based on rule
- Local Server at Intersection: The system must run on a Commercial Off the Shelf Server (COTS). Outdoor IP 66 Quad core processor based server should be able to cover at least 8 lanes. Temperature rating of the server should be at least 60 degree.
- Operating system: The system must be based on open platform and should run on LINUX/Windows Operating system.
- The system should be capable of generating a video & minimum 5 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).
- The system should perform ANPR on all the vehicles passing the site and send alert to the command control and communication centre on detection of any Hot-listed
- With the detected number plate text, picture should also be sent of hot listed vehicle. It is highly likely to misread similar alphabets like 7/1/L or 8/B
- The system should have ANPR/ OCR to address the Alpha numerical character of irregular font sizes.
- 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.
- System should be capable of working in ambient temperature range of 0oC to 60oC.
- Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
- The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
- Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically
- Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
- Ability to video recording in base station for 7 days. Automatically overwrite the data after 7 days.
- Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible
- Network Connectivity: Wired/GPRS based wireless technology with 4G and upgradable or batter to be provided

Digital Network Camera: AS per specified in Surveillance Camera Section 4.3.2

5.1.5.1.2.1.3 Red Light Violation Detection (RLVD) System

5.1.5.1.2.1.3.1 Overview

System should have the facility to provide the live feed of the camera at the central command centre. System should generate Alarms at control room software if any signal is found not turning RED within a specific duration of time. The following Traffic violations to be automatically detected by the system by using appropriate technology. The Evidence camera should also be used for evidence snap generation minimum for Red Light Violation, Stop Line Violation, Wrong left turn violation, Wrong direction driving violation.

The system should be capable of capturing multiple infracting vehicles simultaneously in Different lanes on each arm at any point of time with relevant infraction data like Type of Violation, Date, time, Site Name and Location of the Infraction, Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.

The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof : When it violates the stop line and When it violates the red signal.

The system must have in-built tool to facilitate the user to compose detail evidence by stitching video clips from any IP camera in the junction (including but not limited to the red light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be encrypted. The system should interface with the traffic controller to validate the colour of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.

The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time.

5.1.5.1.2.1.3.2 Scope of Work

Over all solution should be able to provide features and capable to fulfil the following requirements:

Free Left Violation – The non-intrusive system should identify the violation where either the Free Left is blocked by other vehicles or violation occurred when no free left is allowed.

- The system should be capable to mark the free left junctions (through exceptions in case fewer number exists)
- In case of blocking the “Free Left”, the system should capture multiple IVD for the vehicles in the front area of the free left blocking the road.
- In case of “No Free Left”, the system should be able to capture multiple IVD’s.

Speed Violations :

- 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.
- The system shall have the provision of setting different speed thresholds for different class of vehicles.
- The speed violations system should be installed on mid-blocks or designated areas as identified during design stage.

Wrong Direction Vehicle Movement – The non-intrusive system should be installed at critical junctions to capture the wrong direction vehicle movement. The system should identify and capture multiple IVD. The E-Challan standard procedure should be triggered.

Recording & display information - The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:

- Computer generated unique ID of each violation
- Date (DD/MM/YYYY)
- Time (HH:MM:SS)

- Equipment ID
- Location ID
- Carriageway or direction of violating vehicle
- Type of Violation (Signal/Stop Line)
- Lane Number of violating vehicle
- Time into Red/Green/Amber
- Registration Number of violating vehicle

The system should start automatically after power failure. The system should have secure access mechanism for validation of authorised personnel.

A log of all user activities should be maintained in the system.

Roles and Rights of users should be defined in the system as per the requirements of the client

In the event that the connectivity to the ICCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re- established automatically. Ability of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis. System should be mounted as per appropriate deign by MSI.

RLVD Application

It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The programme should allow for viewing, sorting, transfer & printing of violation data.

It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.

All outstation units should be configurable using the software at the Central Location.

Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Kanpur Police database structure. It should also be possible to carry out recursive search and wild card search.

The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering).

The application software should be integrated with the E-Challan/Vahaan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by MSI.

Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image.

Components of the architecture must 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.

The evidence of Infraction should be encrypted and protected so that any tampering can be detected.

The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports as per requirement.

- 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).
- Digital Network Camera : AS per specified in Surveillance Camera Section
- On site-out station processing unit communication & Electrical Interface (Junction Box)
- 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.
- Wired/GPRS based wireless technology with 4G and upgradable
- Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking.
- System should be capable of working in ambient temperature range of -10 degree C to 60oC.
- Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
- The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
- Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC
- Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
- Ability of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.
- Direct extraction through any physical device like USB flash drive , Portable Hard disk etc. shall be possible

5.1.5.1.2.1.4 Speed Violation Detection (SVD) System

5.1.5.1.2.1.4.1 Overview

The Speed Violations should be automatically detected by the system by using appropriate sensors technology.

The system should be capable of capturing multiple infracting vehicles simultaneously in defined lanes at any point of time simultaneously with relevant infraction data like:

- Type of Violation
- Speed of violating vehicle
- Notified speed limit
- Date, time, Site Name and Location of the Infraction
- Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.

The system should be equipped with a camera system to record a digitized image or video frames of the violation, covering the violating vehicle with its surrounding.

The system shall provide the No. of vehicles infracting simultaneously in each lane. The vehicles will be clearly identifiable and demarcated in the image produced by the camera system.

The system shall be equipped with IR Illuminator to ensure clear images including illumination of the number plate and capture the violation image under low light conditions and night time.

Speed measurement may be made by using non-intrusive technology such as Radar/sensor/camera/virtual based or any other appropriate certified technology. CE and homologation certificate from Ministry of Traffic or equivalent department from respective country of origin, document authenticated by Indian Embassy (to authenticate that systems are legalized and tested for infractions to avoid legal issues) or Certificate from internationally accredited metrology laboratories (approved for speed calibration) is acceptable

The system should automatically reset in the event of a program hang up and restart after power failure.

Ability to define role based access

The data shall be transferred to the ICCC in real time for verification of the infraction and processing of challan.

In the event that the connectivity to the ICCC is not established then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically.

Speed Violation Application

It should be capable of importing violation data for the Operator for viewing and retrieving the violation images and data for further processing. The programme should provide for sort, transfer & print command.

It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its web link on notices for court evidence.

All outstation units should be configurable using the software at the Central Location

Violation retrieval could be sorted by date, time, location and vehicle registration number and data structure should be compatible with Kanpur Traffic Police database and Kanpur Transport department database structure.

The operator at the back office should be able to get an alarm of any possible fault(s) at the camera site (outstand) (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering , sensor tampering)

The automatic number plate recognition Software may be part of the supplied system, or can be provided separately as add on module to be integrated with violation detection. a.) Success rate of ANPR will be taken as 80% or better during the day time and 60% or better during the night time on standard number plates.

Image zoom function for number plate and images should be provided. Any updates of the software available, shall be updated free of cost during the contract period by the vendor and will integrate the same with existing application and database of Kanpur Traffic Police and Kanpur Transport department.

The application software should be integrated with the notice branch software for tracing the ownership details of the violating vehicle and issuing/printing notices.

Various users should be access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc.

Apart from role based access, the system should also be able to define access based on location.

Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access

Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of Kanpur Police. The system shall support vertical 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. Main technological components requiring scalability are Storage, Bandwidth, Computing Performance (IT Infrastructure), Software / Application performance and advancement in proposed system features.

The system shall also support horizontal scalability so that depending on changing requirements from time to time, the system may be scaled horizontally.

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 shall 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.

The architecture must 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 Anti- virus mechanism. There shall 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 shall be properly stored & archived for future analysis and forensics whenever desired.

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 growth of the environment.

System shall use open standards and protocols to the extent possible

The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.

The data provided for authentication of violations should be in an easy to use format as per the requirements of user unit.

User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).

Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.

Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).

Image should have a header and footer depicting the information about the site IP and violation details like viz. date, time, equipment ID, location ID, Unique ID of each violation, lane number, Registration Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behaviour is recorded viz. (Speed of violating vehicle, notified speed limit, Speed Violation with Registration Number Plate Recognition facility. Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well

Number plate of cars, buses/HTVs should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.

Interface for taking prints of the violations (including image and above details).

5.1.5.1.2.1.4.2 Scope of Work

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).

General requirements-

The system should be designed to detect both reflective and non-reflective types of license plates.

The system should provide a disaster recovering mechanism including automatic restart function after system failure.

All cameras captured images and other data should be digitally watermarked & encrypted to avoid tampering

- Unit of Speed Measurement Kmph
- Speed detection system to Capture speed 200Kmph ± 5%
- Speed Threshold (Vendor should provide manufacturer certificate/ third party test report in support of their claim)
- Speed Enforcement Technology Radar/Laser/Others
- Digital Network Camera
- Day/Night Mode Colour, Mono, Auto

Local storage: 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.

- Protocol IPV4, IPV6, HTTP, HTTPS, FTP/SMTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, UPnP, NTP, QoS, ONVIF, Profile S
- Security Password Protection, IP Address filtering, User Access Log, HTTPS encryption
- Operating conditions 0 to 50°C (temperature), 50 to 90% (humidity)
- Casing NEMA 4X / IP-66, IK10 Rated
- Intelligent Video Motion Detection & Tampering alert
- Alarm I/O
- Certification UL/EN, CE,FCC

The system should be capable of recording the following details of the infracting vehicles

Computer generated unique ID of each violation

- Date (DD/MM/YYYY)
- Time (HH:MM:SS)
- Equipment ID
- Location ID
- Carriageway or direction of violating vehicle

In cases when multiple infracting vehicles are detected in one instant the system should be capable to provide the following data for all Infracting vehicles detected

- Type of Violation

- Notified speed limit (in Kmph)

Speed of violating vehicle (in Kmph)

- Lane Number of violating vehicle
- Registration Number of violating vehicle

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.

Network Connectivity : Wired/GPRS based wireless technology with 3G upgradable to 4G capability.

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.

The system should be capable of working in the temperature as per city condition

At-least one hour UPS power back up to keep the system functional in case of power failure without any break in recording the violation.

The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).

Violation Transmission and Security

- Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the ICCC electronically through GPRS based wireless technology with 3G upgradable to 4G or wired connectivity, in Jpeg format.
- Advanced Encryption Standard (AES) shall be followed for data encryption on site and ICCC, and its access will protected by a password.
- The vendor shall ensure that the data from the onsite processing unit shall be transferred to ICCC within one day.

Video Recording

- 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 be noted that at any point of time the local storage at the base station should have the data of previous 7 days.
- Direct extraction through any physical device like USB, Hard disk shall be possible.

5.1.5.1.2.1.5 Traffic Accident Reporting System (TARS)

TARS solution should provide:

- Accident reporting system
- Accident recording system
- Analysis of accidents
- Dissemination of data

Solution shall provide accident database that will support collecting high quality information on all aspects of road traffic collisions and incorporate best practices of Road Accident Investigation.

Solution shall support authorities in quickly and accurately reconstructing collisions and analysing the data to develop standards to prevent future collisions or mitigate injuries.

Solution shall support information gathering and dissemination as per various stakeholder requirements for accident data, namely, KSCL, police, decision makers etc.

Information to be captured shall include, but not limited to:

- how the accident happened,
- detailed information about the vehicle(s) involved
- type and extent of human impact
- human factors involved (inebriation, etc.)
- nature of any injuries,
- type and extent of property damage,
- socio-economic data of the people involved,
- primary & secondary causes of the accident
- incident photos
- drawing of accident analysis
- • information on analysing agency and personnel

5.1.5.1.2.1.6 Traffic Sensors Lights and Signals

Appropriate camera based traffic sensors may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined.

Appropriate controller technology may be chosen to provide the operational levels and accuracy as required for successful function of the ATCS system as per the SLAs defined. The proposed traffic controller shall be disabled friendly and shall also provide audio tones output

Traffic Lights: Key Features:

a. lowest power consumption for all colors
b. Meets or exceeds intensity, color and uniformity specifications
c. Temperature compensated power supplies for longer LED life
d. Uniform appearance light diffusing
e. Should be Intertek/ETL/EN certified
f. LED shall be single source narrow beam type with clear lens & Luminance uniformity of 1:15
g. Pedestrian traffic lights should be
h. provided with clearly audible signals for the benefit of pedestrians with visual impairments
i. Phantom Class 5 or equivalent. IP Rating: IP65
j. LED aspects:
k. Red, Amber, Green-Full (300 mm diameter) : Hi Flux
l. Green-arrow (300 mm diameter): Hi flux
m. c. Animated Pedestrian-Red and Green Animated c/w countdown (300 mm) Hi Brite with diffusions
n. LED Retrofit Specifications:
o. Power supply: Redundant
p. Standards: EN 12368 certified
q. Convex Tinted Lens: Available
r. Fuse and Transients: Available
s. Operating Temperature Range: 0 degree Celsius to 55 degree Celsius Turn Off/Turn On Time: 75 milliseconds max

t. Total Harmonic Distortion: <20%

u. Electromagnetic interference: Meets FCC Title 47,Subpart B, Section 15 Regulation or equivalent EN/IRC standard

v. Blowing Rain/Dust Spec: MIL 810F or Equivalent EN/IRC standard complaint

w. Minimum Luminous Intensity (measured at intensity point)(cd):
   - Red 400
   - Amber 400
   - Green 400
   - Dominant Wavelength (nm):
   - Red 630
   - Amber 590
   - Green 490

x. Lamp conflict compatibility system: Compatible with lamp failure and conflict detection

Countdown Timer :

CPU: Micro Controller

Mechanical Specifications

Structural Material Polycarbonate strengthened against UV rays

Body Color: Light Grey/Black

Dimensions:360mm x 370mm x 220mm

Display Specification:

Lamp Diameter : 300mm

Digit Height:150 -165mm

Display Type Dual Coloured (Red & Green)

No. of Digit : 3

LED Specifications

LED Diameter :5mm LED

Viewing Angle 30°

LED Wave Length 630-640nm (Red), 505nm - 520nm (Blue-Green)

LED Dice Material AlInGap (Red), InGaN (Blue-Green)

LED Warranty period 5 years

Poles for Traffic Signals : Material: GI Class ‘B’ pipe

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.

1.No’s of cores: 7 and 14 core 1.5 sq. mm.; 3 Core 2.5 sq. mm.

2.Materials: PVC insulated and PVC sheathed armoured cable with copper conductor of suitable size.

3.Certification: ISI Marked

4.Standards: Indian Electricity Act and Rules

5.IS:1554 - PVC insulated electric cables (heavy duty)

5.1.5.1.2.1.7 NVR (Network Video Recorder):

#	**Description**
1.	The Network Video Recorder (NVR) will be connected via a Gigabit Ethernet network.
2.	NVR shall be of N+N configuration with RAID 6 configuration.
3.	All equipment shall be designed to provide a usable life of not less than 10 years.
4.	The NVRs shall have a self-diagnostic feature including disk status, CPU usage, motherboard temperature, network status and fan status.
5.	The NVRs shall be support interface using 10/100/1000BaseTX. It shall support a total throughput of at least 700 Mbps. The NVR shall be powered using 100-240VAC/50Hz. TR 4.32.
6.	The NVR shall support both Linux and Windows platform.
7.	The NVR shall be capable of digitally signing stored video and digitally sign exported video to ensure chain of trust.
8.	The NVR shall have failover and redundancy built in with seamless playback without manual intervention.
9.	The NVR shall support a minimum of 200 recorded video streams and 20 playback streams with minimum playback of 400 Mbps.
10.	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.
11.	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
12.	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

5.1.5.2 CCTV Surveillance System

MSI has to supply, install, commission and maintain the required number of camera in the location as mentioned in Annexure. MSI has to provision for poles, switch, UPS and other equipment for installing the camera. The MSI should do necessary cabling for electrical supply and connectivity required for the field devices. MSI will also implement the following software to enable monitoring through the surveillance cameras. To facilitate the VMS system architecture, the BIDDER shall ensure that sufficient capacity is designed into the data communications & telecommunications infrastructure to deliver the required functionality, along with the ability to allocate and reserve resources (including bandwidth). Video Management System (VMS) and Video Analytics System. General specification of all type of cameras are as below:

- All the network cameras supplied must be certified for: FCC ,CE and UL (Certificates to be enclosed)
- Ability to have In-house Processor for Bandwidth Compensation & Optimization and Support 3rd Party Edge Analytics, with continuous Learning
- Ability to support use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
- Ability to provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
- The Camera shall support IEEE 802.1X authentication, Password protection, IP address filtering, HTTPS encryption, Digest authentication, User access log, Centralized certificate management
- Ability to support open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications. It should have standard components and proven technology using open and published protocols and adopt to industry established standards.
- The implemented API shall be standardized and supported by all network video products offered by the various manufacturer
- Ability to provide 24/7/365 availability and use.
- All the major components of the CCTV systems shall be latest but field-proven and shall not be End-of-Life / Outdated; the same shall have to be supported by concerned OEM for at-least 5 years' period from the date of supply.
- All the cameras shall have 5 Years OEM warranty and the same shall be submitted on OEM Letter head.
- OEM of CCTV should be registered in India for Last 5 years directly ant not through distributor or Joint Venture. Proof of the same should be attached with the Technical bid.
- OEM of CCTV shall have local Support centre.
- All the cameras shall have ability to change the GOP/ GOV for Bit rate optimization.
- All Fixed cameras shall have ability to select user defined shape for motion detection to include or exclude area to reduce false alarms, bandwidth and storage.
- All cameras shall have ability to send and receive triggers to perform any action without intervention of VMS.

5.1.5.2.1 Overview

City Safety and Security solution helps protect cities against crime, terrorism, and civil unrest, planning events, monitoring of infrastructure, encroachments etc. It helps law enforcement monitor public areas, analyze patterns, and track incidents and suspects enabling quicker response. Keeping the above perspective, KSCL for this purpose is intending to implement the high definition IP based surveillance cameras across various locations within KSCL. The exact location will be finalized after detailed survey by the Concessioner, post award of the contract. The cameras should be housed on the intelligent/street poles. It shall also be possible to adjust the camera focus from a remote location.

Following is an indicative scope of work;

a. Installation and commissioning work includes installation of all required DVRs, cameras, monitors, cables laid in PVC conduit etc., commissioning all the systems at the pre-defined locations in the project area
b. The MSI shall prepare the final camera distribution plan at all the camera locations in discussion with KSCL
c. Actual location for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum coverage
d. Bidder should use the industry best practices while positioning and mounting the cameras. Some of the check-points which need to be adhered by the Bidder while installing / commissioning cameras are as follows:
    - Ensure Project objectives are met while positioning the cameras, creating the required field of view
    - Ensure appropriate housing is provided to protect camera from the on field challenges
    - Carry out proper adjustments to have the best possible image
    - Ensure that the pole /tower/ mast implementation is vibration resistant
    - During implementation period, in case any camera is damaged by a vehicular accident (or due to any other reason outside the control of Bidder) and needs repair, then the MSI will need to repair / have the new camera within 15 days of the incidence. Damages are to be borne by MSI in such cases through proper insurance.
e. MSI shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras are brought out on the GIS map. Bidder is required to carry out the seamless integration to ensure ease of use of GIS in the Surveillance System Applications/ Dashboards in Command Control Centres. GIS Base Map shall be supplied and integrated by the MSI at 1:1000 scale or better with all surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. Field survey needs to be done by the MSI. Bidder is required to update GIS maps from time to time
f. Bidder shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMS to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid.
g. MSI will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. the same will be facilitated by KSCL. It is important to mention that a timely communication and required follow-up will be required by the MSI for the clearances.

h. During implementation period, in case the pole is damaged by a vehicular accident (or due to any other reason outside the control of MSI) and needs repair, then the MSI will need to repair / have the new pole within 15 days of the incident. Damages are to be borne by MSIs in such cases through proper insurance.

i. For the successful commissioning &operation of the edge devices and to provide the video feeds to Command Control Centre, the MSI will be required to provide electricity to the edge devices through the aggregation points. MSI has to plan the power backup based upon the power situation across the city. MSI may propose solar based powering systems however field devices shall be operational 24x7 and power needs to be calculated accordingly.

j. MSI will be responsible for the solution deployment / customization for implementing end-to-end Surveillance System including its integration with other components as required.

k. MSI will ensure that the best practices for software development and customization are used during the software development/customization and implementation exercise.

5.1.5.2.2 Scope of Work

MSI will have to implement CCTV surveillance solution using below minimum requirements or provide batter specification as per city

5.1.5.2.2.1 Video Management System (IP Based)

Functional Requirement:

1. Ability to use centralized management system of all field devices, servers and client installed at KSCL and run on any PC and Operating system.
2. Ability to integrate with ICCC platform and non-proprietary with perpetual license using open standards
3. Ability to view live video stream by user authorization.
4. Ability support a distributed architecture with no single point of failure
5. Dockable windows shall include:
   - Site Explorer
   - Alarms/Events window
   - PTZ and advanced telemetry functions
   - Monitors window
   - Maps window
6. Ability to stream direct from camera to client; streaming via a proxy, or intermediate server.
7. Ability to handshake between client and camera shall be done directly.
8. Ability to provide flexible rule-based system driven by schedules and events.
9. Ability to support IP cameras, Virtualization, Video analytics and storage technologies from major vendors for integration.
10. Ability to support LDAP (Lightweight Directory Access Protocol)l integration
11. Ability to deploy in High availability environment
12. Ability to overlaid cameras in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking in the camera location on the graphical map.

Minimum Technical Specification:

S.No	Features	Specifications
1	Supported Operating Systems	Linux, Microsoft Windows: 7/8, Microsoft Server 2008 R2/2012, Microsoft Windows Embedded 8 Standard. Support for both 32-bit (x86), 64-bit (x64) versions
2	ONVIF Support	ONVIF, ONVIF Profile S Supported Cameras
3	Video Stream Formats	MJPEG, MPEG-4, H.264
4	Audio Support	2-way support
5	Resolution	Limited only by the camera
6	Frame Rate	Limited only by the camera
7	Number of servers in the system	Unlimited
8	Number of remote workstations	Unlimited
9	Interface Language	English and multi-language support
10	Archive Materials Storage Format	In the format received from the IP camera
11	Archive Size	Should be able to create different archive sizes per any camera or any group of cameras.
12	File Playback Speed	From single-frame playback up to 32x speed up or better
13	Auto Zoom	Displaying the separate enlarged area with moving objects
14	PTZ cameras	Control of PTZ cameras using the client interface: camera rotation, zoom in/out (optical zoom), focus
15	Panoramic camera support	Support of various modes used in panoramic cameras with just a single VMS license.
16	Cameras auto search	The ability to automatically search for cameras that support ONVIF or UPnP detection protocol in a local network
17	Server backup	Hot backup: in case of server failure, recording is redirected to a backup server
18	Integration with 3rd Party Video Analytics Server	Should support and accept notifications from 3rd Party analytics server.
19	User Interface	Timeline based UI which allows one-click based access to past recordings.
		Timeline should always accessible. No separate interface for viewing recordings.
		Dragging the timeline should synchronize all camera images to the selected point in time.
		The timeline can be hidden so that the camera windows can be shown on the whole screen.
		Camera window cloning enables the simultaneous viewing of real-time and recorded image.
		VMS should support Calendar search and specific time search
		The size and layout of camera windows should be able to be freely adjusted
		Window layouts should be able to be saved in shortcut buttons with specific labels

		Automatic arrangement of camera windows should be possible
		Video Wall support and camera window arrangement functionality
		Pre-programmable notifications
		Creation and naming of bookmarks of video.
20	Camera Window Tools	Full screen Mode: Should be able to the selected camera in full screen mode
		Create video clip: Should be able to create a video clip recording of the visible image. Can be selected in another camera window, which will cause the video clip to continue from that window. (editable video clip)
		Quick search from this camera: Should only show the recordings for this camera on the timeline. The playback should jump over motion detections in other areas.
		Area search: User should be able to draw areas comprising one or more camera image, and the motion detections of this area will be shown on the timeline. The playback will jump over motion detections in other areas.
		Clone window: Should copy the camera window. Should allow simultaneous viewing of the present time and recordings from the same camera with the use of the “Detach from the main timeline” function.
		Detach from the main timeline: Should open a separate timeline as a window. The other camera windows should follow the main timeline.
		Start recording: Should starts a continuous recording of 1 minute (time adjustable) of this camera image on 1-click.
		Customized buttons: Can be used to control gates or other external devices with rule-customized buttons.
		Screenshot: Saves the visible image as an image file (JPG, PNG or PDF). Resolution can be selected.
21	Remote Use	Compatible with Windows, Linux and OS X client machines
		Should use TCP/IP connection that can be encrypted.
		Can be connected to multiple network video servers simultaneously.
		Recordings from multiple servers can be synchronized.
		Real-time image and recording transfer online, either full quality or compressed quality can be selected.
		Notification events and alarms are forwarded directly from the server to the user.
		Customized buttons enable the management of different functions, such as recording and saving from connected external devices.
22	Notifications	Real-time notification window
		Notifications include a screenshot and a description of the event contents
		Notification colors should be adjustable
		Clicking the notification should open an image recording of the event from the connected camera.
		Bookmarks should be able to be saved directly from notifications
		Should have the capability to have the notification list length of upto 100
		Rules should be able to be used to set specific conditions for notifications.
23		Should support viewing synchronized real-time and recorded image feed from multiple servers

	Multiple Network Video Recorders Synchronization	Should support saving views comprised of camera feed from multiple recorders
		Area search for a combination of cameras from different recorders
		Notifications and alarms from multiple recorders simultaneously
		Saving merged backup copies and video clips
24	Bookmarks	Support saving bookmarks in the timeline
		Support naming, editing and removing bookmarks
		Bookmarks should be saved in the bookmark list and should also be visible on the timeline.
		Bookmarks are saved locally.
		Bookmarks can be browsed with the arrow keys, previous/next
25	Editable Camera Views	Camera windows can be arranged as wanted
		Camera window layouts can be saved and named
		Frequently used views can be saved as shortcut buttons
		Camera views can contain cameras from multiple recorders
26	Video Clips	Time frame and selected cameras: Saves a grid comprising of selected cameras into a single file.
		Quick search and area search can be used with the video clip tools.
		Save as an AVI/MP4 .
27	Backup Copies	Saving of full-quality backup copies
		The start and end points of the backup file can be freely determined.
		Quick search and area search can be used to filter unwanted movement.
		Backup copies can be viewed using the remote software.
		Quick and area searches can be made in the backup file
		Video clips and screenshots can be saved from the backup file.
28	Rules	Rules can be used to control recorder functionality and external devices as well as to send information on different events
		One or more conditions are set for the rules.
		Conditions can include for example: Schedule, I/O-feed, motion detection, alarm lines, connection loss etc.
		Rules are set actions to be performed when rule conditions are met. Actions can include: Digital output control, notification event/alarm, selecting a PTZ preset, saving a bookmark, sending an email message etc.
29	User Management	Username and password protection, Selecting functions and software areas, Camera access based on user permissions, Remote access selection for users, Camera control selection for users
30	Archival Storage Modes	Storage space is shown as a percentage of total available space.
		Recording time can be specified to a date.
		User Interface should be able to show the date of the oldest recording
31	Access Groups and Users	The VMS should have the capability to create atleast 4 access groups.
		Administrator should have the right to assign the camera to atleast one group.
		Different level of access to the camera shall be configurable in the VMS
32	Tab switch	Tab switching time should be configurable from 1 sec to 60 sec for allowing all the cameras to appear on screen tab wise , tab switch time should be common to all the tabs

33	Software Motion Detection	Smart Motion detection should function with all types of ONVIF conformant cameras regardless of manufacturer.
		Sensitivity and noise reduction should be adjustable.
		VMS Should index the location of motion in the image for the purposes of area searches.
		Separate motion detection areas with different sensitivity can be set for an image.
		Areas of the image that should not be recorded can be covered via motion detection.
34	Map View	Cameras can be placed in map views and opened directly from the map
		There can be multiple maps e.g. for different floors.
		Maps can include links to other maps.
		Maps are placed in separate movable windows, and several windows can be viewed simultaneously
		Maps can be zoomed and moved by using your mouse inside the window.
		Camera locations can be edited
		Map modification can be turned off
35	Virtual Matrix	Command and Control room interface for real-time surveillance
		Virtual matrix can include one or more screens and should support Video Walls.
		Includes monitor windows and regular camera windows that can be used to record several views
		Image source selection for monitor windows can be automated e.g. based on alarms.
		Cameras selected for monitor windows can be controlled with one or more joysticks.
		Controlled camera can be selected with joystick buttons or mouse.
		Notification events are shown instantaneously from e.g. alarm information or motion detection.
36	Shortcut keys	VMS should have the option of customizing the shortcut keys.
37	Diagnostics	Notification events can be set in the system in different ways, such as rules, motion detection from image, external I/O data, or internal software command.
		Notifications can contain a free text field, event colours are customisable, and a preview image is attached to the notification.
		Status information and preset alarms are saved in the alarm log in chronological order
		The alarm log contains an acknowledgement functionality.
		User can access a recording attached to a notification by one click
38	System	VMS and CCTV cameras maybe from same OEM

5.1.5.2.2.2 Outdoor/Fixed Box cameras (High Definition)

S.No	Features	Specifications
1	Form Factor	Box Type
2	Image Sensor	1/2.8" Progressive CMOS
3	Day/ Night Operation	ICR
4	Minimum Illumination	Color 0.04 lux , B/W 0.002 lux

5	Lens	External Lens (5 mm to 50 mm)
6	Electronic Shutter	1 ~ 1/10000 sec.
7	Image Resolution	3M (2048x1536) or better
8	Compression	H.264 , MJPEG
9	Frame Rate and Resolution	H.264 3M (2048 X 1536) @25/30 fps , 2 MP (1920 X 1080) @ 50/60 FPS
	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
10	White Balance	Auto / Manual / ATW / One Push
11	Noise Reduction	3DNR / 2DNR / ColorNR
12	Zoom	Digital Zoom
13	Video Streams	Quad Stream supportable , All stream should be H.264
14	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
15	Two way audio	Line in / Line out
16	Audio Compression	G.711 / G.726 / AAC / LPCM
17	Iris	P – iris
18	Wide Dynamic Range	120 dB
19	Alarm	2 x Input / 1 x output
20	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal
21	Network Interface	1 x RJ45
22	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
23	Protocols	ARP, IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
24	Text Overlay	Date & time, and a customer-specific text etc
25	Security	HTTPS / IP Filter / IEEE 802.1X
26	Firmware Upgrade	The firmware upgrade shall be done though web interface, the firmware shall be available free of cost
28	Video Output	1 X BNC
31	Power	PoE / DC 12V / AC 24V
32	Operating Temperature	,-30°C ~ 60°C
33	Operating Humidity	,10% ~ 90%, No Condensation
34	Certification	UL , CE , FCC
35	ONVIF	ONVIF profile S & G
36	User accounts	20
37	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari

S.No	Features	Specifications
1	Form Factor	Dome
2	Image Sensor	1/2.8" CMOS or better
3	Day/ Night Operation	Yes with IR Cut Filter
4	Minimum Illumination	Color 0.04 lux ,B/W 0.002 lux
5	Lens	3 - 9 mm, P-Iris, Megapixel Lens with remote zoom and focus
6	Electronic Shutter	1 ~ 1/10,000 s
7	Image Resolution	3 MP or better
8	Compression	H.264 , MJPEG
9	Frame Rate and Resolution	H.264 3M (2048 X 1536) @25/30 fps , 2 MP (1920 X 1080) @ 50/60 FPS
10	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11	White Balance	Auto / Manual / ATW / One Push
12	GOV Length	It should be possible to vary the GOV length in the camera setting .
13	Noise Reduction	Digital Noise Reduction 2D / 3D DNR
14	Zoom	3x optical Zoom , 10x Digital Zoom
15	Digital PTZ	Camera should support digital PTZ
16	Video Streams	Quad Stream supportable , All stream should be H.264
17	Video quality view	Video compression type (H.264/MJPEG) and bit rate of each stream should be viewable on home screen
18	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
19	Two way audio	Line in / Line Out
20	Audio Compression	G.711 / G.726 / AAC / LPCM
21	Iris	P iris
22	Wide Dynamic Range	120 dB or better
23	IR	Upto 40 mtr IR distance
24	Alarm	1 x Input / 1 x output
25	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal
26	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
27	Network Interface	RJ-45, 10/100Mbps Ethernet
28	Edge Storage	Built in SD card slot with support upto 128 GB SD card
29	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
30	Text Overlay	Date & time, and a customer-specific text etc
31	Security	HTTPS / IP Filter / IEEE 802.1X
32	Firmware Upgrade	The firmware upgrade shall be done though web interface,
33	Video Output	1 X BNC
34	Enclosure	IP 66 weather proof ,
35	Vandal Resistant	IK 10
36	Power	POE / 12 V DC /24 V AC
37	Operating Temperature	As per City requirement

38	Operating Humidity	Humidity 10%–90% No Condensation
39	Certification	UL, CE, FCC, RoHS
40	ONVIF	ONVIF Profile S & G
41	User accounts	20
42	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari or similar or higher browser

Sr No	Parameters	Minimum Specifications
1	Image Sensor	1/2.8” progressive scan RGB CMOS
2	Day/ Night Operation	Yes with IR Cut Filter
3	Operating Frequency	50 Hz
4	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W": 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 50 Meters
5	Low light Capability	The camera shall be able to provide usable Color video in low light conditions
6	Lens	8-50mm IR corrected, CS-mount lens, P-Iris
7	Electronic Shutter	1/28000 s to 2 s or better
8	Image Resolution	1920 x 1080, 1280 x 720, 800 x 450, 480 x 270, 320 x 240
9	Compression	H.264 in High and Base profile, MPEG4, MJPEG
10	Frame Rate and Bit Rate	25 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate
11	Video Streams	Minimum 4 Streams in H.264, 2MP, 25 fps
12	Motion Detection	Yes built in with multiple configurable areas in the video stream
13	Pan Tilt Zoom	Digital PTZ
14	Frame Rate and Bit Rate	Upto 50 fps at all resolutions
15	Electronic Exposure & Control	Automatic/ Manual
16	Wide Dynamic Range	120 dB or better
17	Backlight Compensation	Required
18	Privacy Masks	Minimum 20 configurable 3D zones
19	Connectors	1 Input & 1 Output for Alarm Interface
20	Audio	Two way Audio

21	Event Triggers	Intelligent video, Edge Storage event, External Input, Audio Level, Motion Detection, Day/Night Mode, Network, Time scheduled, 3rd Party Analytics, Manual Trigger, Alarm Input Trigger
22	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP PTZ function, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, External Output activation
23	Edge Storage	Built in SD card slot with support upto 128 GB with Class 10 speed
24	Built in installation aids	Focus assistant, Pixel counter, Remote back focus
25	Storage	The Cameras shall have the feature to directly record the videos/ images onto NAS/SAN without any Software or integration
26	Protocols	IPv4/v6, HTTP , HTTPS b, SSL/TLS b, QoS Layer 3 DiffServ, FTP , CIFS/SMB, SMTP, Bonjour, UPnP™,SNMPv1/v2c/v3 (MIB - II), DNS, DynDNS, NTP, RTSP, RTP,TCP, UDP,IGMP,RTCP,ICMP,DHCP,ARP,SOCKS
27	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc
28	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
29	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost
30	Logs	The camera shall provide minimum 200 logs of latest connections, access attempts, users connected, changes in the cameras etc
31	Interface	RJ 45, 100 Base TX
32	Enclosure	IP66-and NEMA-4X-rated casing (polyester polycarbonate blend)
33	Power requirements	Vendor to Specify
34	Operating Temperature	-20 °C to 55 °C
35	Operating Humidity	Humidity 10–95% RH (condensing)
36	Certification	UL, CE, FCC, IEC
37	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
38	Housing, Mount and IR	Shall be of the same make of OEM or better
39	Onvif S	Required

5.1.5.2.2.3 Pan, Tilt and Zoom cameras (PTZ)

S.No	Parameters	Specifications
1	Certifications	UL ,CE,FCC
2	Compatibility	ONVIF profile S , G and Q
3	Sensor	1/2.8" Progressive CMOS
4	Resolution	3 MP (2048 X 1536)
5	Multiple Stream	Quad Stream
6	Frame Rate	upto 30 fps @ 3MP , upto 60 fps @ 2 MP
7	Focal Length	4.3-129 mm
8	Field Of view	64° - 2.4 °
9	Optical Zoom	30X
10	Digital Zoom	10X
11	Focus	Auto / Manual
12	WDR	120 dB
13	Noise Reduction	2D / 3D
14	Shutter Speed	1/1 ~ 1/10000 sec.
15	IR	Inbuilt IR , IR distance upto 150 mtr
16	Day & Night	IR Cut filter
17	Min Illumination	0.05 @ F1.6 (Color), 0 (B/W) @ F1.6
18	Iris	P iris
19	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal
20	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
21	Edge Storage	Built in SD card slot with support upto 128 GB SD card
22	Video Compression	H.265,H.264
23	Privacy Mask	upto 20 privacy zones
24	PTZ	DSCP Protocol Support
25	Audio	2 Way audio
26	Audio Compression	G.711 / G.726 / AAC
27	PAN	360 ° endless , Manual speed 0.1° ~ 90°/s , preset speed 9° ~ 280°/s
28	Tilt	,-20° ~ 200° , Manual speed 0.1° ~ 60°/s , Preset speed 7° ~ 300°/s , Auto flip
29	Presets	256
30	PTZ Operation	8 sequence , 8 cruise
31	Speed by zoom	On / Off (Pan and tilt speed proportional to zoom ratio)
32	Home Function	Preset / Sequence / Auto pan / Cruise
33	Calibration	Auto(On/Off)
34	Resume after power loss	Supported zero downtime power switching

35	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF, ARP
36	Security	HTTPS / IP Filter / IEEE 802.1x
37	Alarm	4 Input / 2 Output
38	Alarm response	Preset / Sequence / Auto Pan / Cruise
39	BNC	1 X BNC
40	Ethernet Interface	1 X RJ 45
41	Supported Web browser	Internet Explorer (10.0+) / Firefox / Safari or similar or higher browser
42	Weather Proof	IP 66
43	Operating Temperature	As per city Requirements
44	Power Supply	802.3at (PoE+) 4-Pair 60W / AC 24V ± 20% / DC 12V
45	Power Consumption	45W or less (with IR & Heater on)

5.1.5.2.2.4 Fixed Camera with Outdoor Housing and Lens – 2MP

S.No	Features	Specifications
1	Form Factor	Dome
2	Image Sensor	1/2.8" CMOS or better
3	Day/ Night Operation	Yes with IR Cut Filter
4	Minimum Illumination	Color 0.04 lux ,B/W 0.002 lux
5	Lens	3 - 9 mm, P-Iris, Megapixel Lens with remote zoom and focus
6	Electronic Shutter	1 ~ 1/10,000 s
7	Image Resolution	3 MP or better
8	Compression	H.264 , MJPEG
9	Frame Rate and Resolution	H.264 3M (2048 X 1536) @25/30 fps , 2 MP (1920 X 1080) @ 50/60 FPS
10	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
11	White Balance	Auto / Manual / ATW / One Push
12	GOV Length	It should be possible to vary the GOV length in the camera setting .
13	Noise Reduction	Digital Noise Reduction 2D / 3D DNR
14	Zoom	3x optical Zoom , 10x Digital Zoom
15	Digital PTZ	Camera should support digital PTZ
16	Video Streams	Quad Stream supportable , All stream should be H.264
17	Video quality view	Video compression type (H.264/MJPEG) and bit rate of each stream should be viewable on home screen
18	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
19	Two way audio	Line in / Line Out
20	Audio Compression	G.711 / G.726 / AAC / LPCM
21	Iris	P iris
22	Wide Dynamic Range	120 dB or better

23	IR	Upto 40 mtr IR distance
24	Alarm	1 x Input / 1 x output
25	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal
26	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
27	Network Interface	RJ-45, 10/100Mbps Ethernet
28	Edge Storage	Built in SD card slot with support upto 128 GB SD card
29	Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
30	Text Overlay	Date & time, and a customer-specific text etc
31	Security	HTTPS / IP Filter / IEEE 802.1X
32	Firmware Upgrade	The firware upgrade shall be done though web interface,
33	Video Output	1 X BNC
34	Enclosure	IP 66 weather proof ,
35	Vandal Resistant	IK 10
36	Power	POE / 12 V DC /24 V AC
37	Operating Temperature	-30 °C to 60 °C
38	Operating Humidity	Humidity 10%–90% No Condensation
39	Certification	UL, CE, FCC, RoHS
40	ONVIF	ONVIF Profile S & G
41	User accounts	20
42	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari or similar or higher browser

5.1.5.2.2.5 ANPR/RLVD Camera

S.No	Features	Specifications
1	Form Factor	Box Type
2	Image Sensor	1/2.8" Progressive CMOS
3	Day/ Night Operation	ICR
4	Minimum Illumination	Color 0.04 lux , B/W 0.002 lux
5	Lens	External Lens (5 mm to 50 mm)
6	Electronic Shutter	1 ~ 1/10000 sec.
7	Image Resolution	3M (2048x1536) or better
8	Compression	H.264 , MJPEG
9	Frame Rate and Resolution	H.264 3M (2048 X 1536) @25/30 fps , 2 MP (1920 X 1080) @ 50/60 FPS
	Simultaneous Stream	Minimum 2 streams should be configurable at 1920 X 1080 @ 25 fps simultaneously
10	White Balance	Auto / Manual / ATW / One Push
11	Noise Reduction	3DNR / 2DNR / ColorNR
12	Zoom	Digital Zoom

13	Video Streams	Quad Stream supportable , All stream should be H.264
14	Image Setting	Saturation, Brightness, Contrast, Sharpness, Hue adjustable
15	Two way audio	Line in / Line out
16	Audio Compression	G.711 / G.726 / AAC / LPCM
17	Iris	P – iris
18	Wide Dynamic Range	120 dB
19	Alarm	1 x Input / 1 x output
20	Edge Video Content Analytics	Camera should have in-built Edge Bases Analytics, Abandoned Object, Intrusion Detection, Tampering, Wrong Direction, Loitering Detection, Object Counting, Stopped Vehicle, Object Removal
21	Network Interface	1 x RJ45
22	Storage backup on network failure	Camera should support network failure detection , Camera should have the capability to start the recording automatically on SD card in case of connectivity between camera and NVR/Storage device goes down
23	Protocols	ARP, IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
24	Text Overlay	Date & time, and a customer-specific text etc
25	Security	HTTPS / IP Filter / IEEE 802.1X
26	Firmware Upgrade	The firmware upgrade shall be done though web interface, the firmware shall be available free of cost
28	Video Output	1 X BNC
31	Power	PoE / DC 12V / AC 24V
32	Operating Temperature	As per city Requirements
33	Operating Humidity	,10% ~ 90%, No Condensation
34	Certification	UL , CE , FCC
35	ONVIF	ONVIF profile S & G
36	User accounts	20
37	Supported Web Browser	Internet Explorer (7.0+) / Firefox / Safari or similar or higher browser

5.1.5.2.2.6 Infrared Illuminators

The infrared illuminators are to be used in conjunction with the Fixed Box cameras specified above to enhance the night vision.

Sr.NO	Description	Required Parameters
1	Power	Auto on off
2	IR Control	Power level, Photocell sensitivity, Timer
3	Type	850 nm semi-covert
4	Distance & Angle of Beam with Lens Options.	Minimum : 10° x 10°: 120 m (394 ft) 35° x 10°: 65 m (213 ft) 60° x 25°: 45 m (148 ft) 80° x 30°: 30 m (98 ft) or batter
5	Casing	Aluminium and Polycarbonate

6	LED Indicators	Required
7	Environmental Protection	IP66, IK09 Rated
8	Mount Options	Wall, Ceiling, Camera Housing Mount
9	Operating Temperature	-50 °C to 55 °C or batter
10	Warranty	Min 3 Years OEM Warranty
11	Standards/Certification	UL,CE,FCC, EN, WEEE, RoHS
12	Approved Makes	Same as Camera OEM

5.1.5.3 Variable Message Sign boards

5.1.5.3.1 Overview:

i. Central Control Software shall allow controlling multiple VMSB from one console.

ii. Capable of programming to display all types of Message/ advertisement having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content for VMSB display.

iii. The system shall have capability to divide VMSB screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.

iv. The system shall also provide airtime management and billing system for paid content management

v. Capable of controlling and displaying messages on VMSB boards as individual/ group.

vi. Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMSB.

vii. Capable of controlling brightness & contrast through software.

viii. Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network.

ix. Real time log facility – log file documenting the actual sequence of display to be available at central control system.

x. Multilevel event log with time & date stamp.

xi. Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.

xii. Location of each VMSB will be plotted on GIS Map with their functioning status which can be automatically updated.

xiii. Report generation facility for individual/group/all VMSBs 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.

xiv. Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMSB unit.

xv. 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.

xvi. Apart from role based access, the system shall also be able to define access based on location.

xvii. Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access

xviii. Components of the architecture must 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.

xix. The architecture must 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.

xx. 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 growth of the environment.

xxi. System shall use open standards and protocols to the extent possible

xxii. Facility to export reports to excel and PDF formats.

xxiii. Remote Monitoring

   a. All VMSB shall be connected/configured to Traffic Monitoring system for remote monitoring through network for two way communication between VMSB 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.

5.1.5.3.2 Scope of Work

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

i. Variable Message Sign Board (VMSB) referred herein) shall be installed at identified strategic locations. The location of VMSB shall be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMSB software application will allow user to publish specific messages for managing traffic and also general informative messages.

ii.VMSB shall enable KSCL/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.

iii.These displays can also be used for advertisement purposes. Approximately 20% to 30% of the total running time will be utilized by KSCL in day-to-day scenario (i.e. normal, non-emergency situations) for its own discretion whereas the remaining time can be used for advertisement purpose. However during emergency or disaster situations, VMBS would be required to play messages issued by ICCC all the time till normal situation is restored.

<u>System Requirements</u>

The system should be capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the ICCC in real time.

The system should also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops.

The VMSB should display text and graphic messages using Light Emitting Diode (LED) arrays.

The System should be able to display failure status of any LED at ICCC.

The System should support Display characters in true type fonts and adjustable based on the Operating system requirement.

The VMSB workstation at the ICCC should communicate with the VMS 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 VMS workstation should receive status data from the VMS controller.

VMSB controllers should continuously monitor the operation of the VMS via the provided communication network.

Operating status of the variable message sign should be checked periodically from the ICCC.

It shall be capable of setting an individual VMSB or group of VMSB’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.

It shall be capable of being programmed to display an individual message to a VMSB or a group of VMSB’s at a pre-set date and time.

A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMS or group of VMS’s.

It shall also store information about the time log of message displayed on each VMS. The information stored shall contain the identification number of the VMS, content of the message, date and time at which displayed message/picture starts and ends.

The central control computer shall perform regular tests (pre-set basis) for each individual VMS. Data communication shall be provided with sufficient security check to avoid unauthorized access.

Variable Message Sign Board application

Central Control and Communication Software should allow controlling multiple VMS from one console.

Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi, and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display.

The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management

Capable of controlling and displaying messages on VMS boards as individual/ group.

Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMS.

Capable of controlling brightness & contrast through software.

Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the ICCC via communication network.

Real time log facility – log file documenting the actual sequence of display to be available at central control system.

Multilevel event log with time & date stamp.

Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.

Location of each VMS will be plotted on GIS Map with their functioning status which can be automatically updated.

Report generation facility for individual/group/all VMSs 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.

Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMS unit.

Various users should access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.

Apart from role based access, the system should also be able to define access based on location.

Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access

Components of the architecture must 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.

The architecture must 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 Anti- virus 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.

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 growth of the environment.

System shall use open standards and protocols to the extent possible

Solution shall be integrated with the environmental monitoring system for automatically displaying information from environmental sensors.

Facility to export reports to excel and PDF formats.

Remote Monitoring

All VMSB shall be connected/configured to ICCC for remote monitoring through network for two way communication between VMS and control Room to check system failure, power failure & link breakage.

Remote Diagnostics to allow identifying failure up to the level of failed individual LED.

Minimum 3.0m length X 1.5m height X 0.2m depth. (3000mm x 1500mm X 200mm approx)

Colour LED: Full Colour, class designation C2 as per IRC/EN 12966 standard

Luminance Class/Ratio: L3 as per IRC/EN 12966 standards.

Luminance Control & auto Diming

Should be automatically provide different luminance levels but shall also be controllable from the traffic centre using software.

Auto dimming capability to adjust to ambient light level (sensor based automatic control)

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.

Contrast Ratio: R3 as per IRC/EN 12966 standard

Beam Width: B6+ as per IRC/EN12966 standards.

Pixel Pitch: 12mm or better

Picture Display

At least 300mm as per IRC /EN 12966 standards

Full Matrix: Number of lines & characters adjustable, active area: 2.88mX1.2m at-least

Synchronized Dot to Dot display.

Capable of displaying real time message generated by ICCC.

Special frontal design to avoid reflection.

Display shall be UV resistant

Viewing Angle: B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road

Viewing Distance: Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles.

Self-Test

VMS shall have self-test diagnostic feature to test for correct operation.

Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated.

All periodic self-test results shall be relayed to the ICCC in real time to update the status of the VMS

Alarms

Door Open sensor to Inform Control room during unauthorized access

LED Pixel failure detection alarm

Flicker: Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.

Multiple Data Communication interface/Port: RJ45 Ethernet, RS232, RS 485, FC port and any other suitable

Communication (connectivity): Wired & GPRS based wireless technology with 3G upgradable to 4G capability.

Ambient Operating Temperature: should be capable of working in ambient temperature of city requirement

Humidity (RH): Operating ambient humidity: 10% - 95% Rh or better.

Protection against Pollution/dust/water: Complete VMS should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard.

Power

Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.

The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.

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.

Batteries with solar charging options can also be provided as back up

Material for VMS frame: at least 2mm aluminum or Non-corrosive, water resistant or better. Frame of the VMS should be black & Powder coated.

Mounting, Installation and finishes

Mounting structure shall use minimum 6Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.

The mounting shall be capable of withstanding road side vibrations at site of installation.

It shall be provided with suitable walkway for maintenance access.

The side interior and rear of enclosures shall be provided in maintenance free natural aluminium finish. All enclosure shall be flat and wipe clean.

Rugged locking mechanism should be provided for the onsite enclosures and cabinets.

For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.

Wind Load: WL9 as per EN12966 to withstand high wind speeds and its own load.

Cabling, connections and Labelling

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.

All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.

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.

All cables shall be clearly labelled with indelible indication that can clearly be identified by maintenance personnel using “As built: drawings”.

Lightening arrester shall be installed for safety on each VMS.

The successful bidder has to provide safety certificate from qualified Electrical engineers approved/certified by Govt. Agency.

Local Storage in VMS: Embedded VMS 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.

5.1.5.4 Public Address (PA) System

5.1.5.4.1 Overview

i. The Public Address System (PA) shall be capable of addressing citizens at specific locations from the ICCC.

ii. The proposed system shall contain an IP-based announcing control connected to the ICCC.

iii. Public Address system shall be used at intersections, public places, market places or those critical locations as identified by KSCL to make important announcements for the public.

iv. The system shall contain an IP based amplifier and uses PoE power which shall drive the speakers. The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

v. 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.

vi. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.

vii. The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

viii. PA system’s master controller shall have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.

ix. PA system’s master controller should facilitate multiple MIC inputs and audio inputs.

5.1.5.4.2 Scope of Work

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

- MSI shall install IP based Public Address System as part of the information dissemination system at 50 locations (tentative) in the city. These systems shall be deployed at identified junction to make public interest announcements.
- The system deployed shall be IP based and have the capability to be managed and controlled from the ICCC
- MSI, in consultation with KSCL can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in KSCL will be maximized.
- KSCL shall review and approve the proposed locations. MSI shall install the PA system on the approved locations.
- Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously.
- The PAS should also support both, Live and Recorded inputs and have minimum following capability
  - Speaker: Minimum 2 speakers, To be used for Public Address System
  - Connectivity: IP Based
  - Access Control : Access control mechanism would be also required to establish so that the usage is regulated.
  - Integration : With VMS and Command and Control Centre
  - Construction : Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
  - BatteryInternal Battery with different charging options (Solar/Mains)
  - Power Automatic on/off operation
  - Casing IP-55 rated for housing

5.1.5.5 Emergency Call Box (ECB) System

5.1.5.5.1 Over view

A high quality digital transceiver, to be placed at strategic locations determined by the KSCL. Key is to make it easily accessible by public. The unit shall preferably have a Double button which when pressed, shall connect to the ICCC over the existing network infrastructure setup for ITMS project. These are to be placed only at a select locations such as CCTV field of view to avoid misuse and vandalism of the call box.

5.1.5.5.2 Scope of Work

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

i. MSI shall also install Emergency Call Box/Panic buttons at 50 locations (the final no. might vary based on field survey by MSI) in the city. These systems shall be deployed at identified junction for ease of access by citizens of Kanpur city.

ii. MSI, in consultation with KSCL can propose alternate locations apart from the locations mentioned in this RFP for installing ECB system where their effectiveness in communicating information about traffic conditions in KSCL will be maximized.

iii. KSCL shall review and approve the proposed locations. MSI shall install ECB system on the approved locations.

iv. ECB should have minimum following capabilities:

- Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment
- Call Button: Watertight Push Button, Visual Feedback for button press
- Speaker: To be used for Public Address System
- Connectivity: GSM/RF/PSTN/Ethernet as per solution offered
- Sensors: For tempering/ vandalism
- Battery: Internal Battery with different charging options (Solar/Mains)
- Power: Automatic on/off operation
- Casing: IP-55 rated for housing

5.1.5.6 Smart Parking Management System (SPMS)

5.1.5.6.1 Overview:

Lack of sufficient parking space has been a real phenomenon which citizens of KSCL has been facing for long. As of now, there is no multilevel parking available in the city. There are total ~42 designated open parking area in the city and 72 proposed parking areas. The proposed parking lots shall have ~12000 Sq Meter area which can accommodate ~500 cars considering 25 Sq meter per vehicle. Out of these available parking spaces, there has been a need to find real-time information on availability of parking spaces in the city and disseminate this information to commuters. With Smart Parking solution, it is envisaged to have a system that alerts residents where the open parking space is available, provide parking rates and guides them to the parking area.

As part of this RFP, KSCL has decided to going for Smart Parking solution over conventional parking due to the following parameters:

- High Parking Search Time
- Traffic Congestion on Road
- Poor Usage of Parking Space
- Poor Occupancy in Parking Lot
- Less effective parking operations
- High Parking violations
- Accidental Hazards
- Stress to user & dissatisfaction
- Pollution – High Emission of gas
- No real time tracking, data/report for analysis for future need/expansion

Smart Parking Solution

With Smart Parking Management System, residents shall come to know the open parking space available around the city, parking charges, map based guidance and probability of finding a space in the parking based on predictive algorithm. MSI shall assess the existing and proposed street parking places and recommend the parking solutions for the same.

Intelligent parking operators shall have following features;

1. Mobile App to help in finding parking space quickly & easily
2. Finding parking space with clear & simple directions reducing traffic Congestion.
3. Improved Parking Occupancy increase collection
4. Improved user satisfaction by saving time, effort & cost
5. Less parking search time reduces emission of gases & control pollution
6. Correct detections of violations & suspicious parking/over duration parking
7. Availability of data & Analysis for growing need for expansion or more parking slots; subsequently required measures to handle problem

Smart Parking Key Components

1. Parking Sensors
   a. Installation of parking sensors in the allotted space which communicate information wirelessly

2. Wireless Sensor Networks Module
    a. Collect sensor data
    b. Check parking slot state in real-time
    c. Send parking slot information to webserver
3. Web Portal and Mobile App for Public
    a. Connect to central web-server
    b. Receive parking slot information from central web-server
    c. Display the real-time monitoring of parking slots state in the nearest parking zone
4. Control and command center
    a. Integration with ICCC system
    b. Data management, analytics and Business Intelligence on real time basis
    c. Monitoring of real time transactions, parking availability
    d. Management of Equipment status and alarms on real time basis
    e. Dash boards and reports
5. Central Web-Server
    a. Receive parking slot information from wireless sensor networks
    b. Display the parking slots state of parking zone in real-time
    c. Send information to mobile phone application
    d. Save information in SQL database
    e. Reporting & analytics
6. Digital Display Unit
    a. Shall receive information from the Parking Information System and operate accordingly

5.1.5.6.2 Scope of Work

Functional Requirements:

The smart parking solution is envisaged for both closed parking lots and open parking lots.

Indoor Parking Spaces- Such parking spaces are managed by KMC through sub contracted vendors and the parking lots have boundary walls, closed terrace and a defined entry and exit points.

Outdoor Parking Spaces- Such locations are managed by KMC through sub contracted vendors and have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road.

On street Parking Spaces- Such locations are managed by KMC through sub contracted vendors and do not have a boundary wall and defined entry and exit points. These kind of parking spaces have specified number of slots available, typically on an open ground or road

Solution must geo-reference all the parking lots and shall have the ability to add more locations in future.

Solution should be able to tally the entry and exit car counts and calculate the available parking in that parking structure.

Solution may use video camera based analytics or other sensor based solutions to determine number of vehicles entering and exiting parking lots. The smart parking solution should do so at each floor, in case of multilevel parking and communicate the data.

Solution shall also include provision to capture image of vehicle including license plate number of every vehicle entering and leaving any of the parking spaces and the all the information related to the same shall be stored at a central server.

Compliance

a. The smart parking solution should retain videos of car entering /exiting the parking zone as per the security parameters defined by KSCL

b. MSI must ensure that all parking slots are individually and clearly marked. Solution should enable accounting and mapping of individual parking spots. All newly proposed parking spots must have one-to-one mapping with parking sensors. From existing ones, except for the very small ones, all rest will eventually have one-to-one mapping with parking sensor by phase-2 of implementation as suggested in both options of implementation strategy.

c. There should be a provision to increase or decrease the number of parking spaces that can be reserved online through web client or mobile App, and same must reflect on web clients or mobile apps.

Visibility of vacant parking spaces

Total number of slots and free slots for parking must be displayed on a digital signboard , Mobile App, Web portal

Solution should report occupancy of parking lots to a central software application deployed at the Integrated Command and Control Center.

Solution should enable KSCL to obtain real time situational awareness about the occupancy of parking lot through smart dashboard.

- Solution should enable citizens to obtain real time space availability.

Parking Guidance subsystem for motorists

i. Accessibility of real time Parking space availability over Web client and Mobile App

a. The smart parking solution should provide real time location based view to citizens about proximity of parking lots and availability of parking lots.

b. The smart parking solution should have a mobile and a web delivery channel for citizens to get real time parking availability.

c. A mobile application and web based user interface should be provided with the following features:

i. The application should have citizen module and officer module.

ii. The citizen should be able to see all the parking lots with exact available space in a real time mode.

iii. While locating nearest parking lot, the most updated parking slot availability should be given to the user.

iv. Through the citizen module, the user should be able to locate nearest parking lot and also pre –book based on his geographical coordinates. The same information must be made available on map with routing information.

v. Citizens should be able to generate MIS report to view their occupancy of parking lots over a defined time period.

vi. The administrators should be able to generate MIS report to view occupancy, collection and other usage statistics over a defined time period.

Solution should be able to communicate parking availability information at each parking lot on a LCD displays deployed at key points of interest in the city.

The Citizen App and Web Portal shall have module for Parking Solution. Solution should optimally make parking data available to a smart phone application that citizens might use to get real time parking availability.

Vehicle and License Plate Image Capture

□ Solution shall have capability to automatically capture details of the license plates of the vehicles at every entry and exit of each parking lot.

□ Appropriate cameras shall be installed at entry and exit of each Parking Lot.

Real-time Monitoring and Dynamic MIS Reporting

□ System shall include central reporting system establishing the connection between the devices and sensors, and the ICCC.

□ Solution shall include reporting dashboards with location specific thresholds to be set for generating customized reports

□ CannzTolution shall be capable of monitoring the number of vehicles that entered or exited the parking premises during any given time

□ Reports shall be available in all standard acceptable formats like .csv, .pdf, .txt, etc.

Sr.No	**Minimuim Functional Requirement**
	Parking Management & Guidance System
1.	Mobile Point of Sale (MPOS) • Wireless Handheld Entry & Exit Device with Integrated Bluetooth/Micro USB Printer • The device should be android powered • The POS device should be able to control boom barrier via Bluetooth or Wi-Fi. • The POS device should be able to store atleast 6 months of data • The shift reports could be collected from the POS devices itself • The POS device should work offline as well, store relevant data in SD Card and the data stored from offline operation should be synced with the server as soon as connection is restored • The barriers should be functional even in offline mode

	• The printer shall be connected with the POS terminal via Bluetooth or micro USB or POS device shall have an integrated printer • The POS device should have an integrated 1D & 2D bar code scanner • Device should be an online unit, connected in real-time with Parking Operations control center through Wi-Fi and 2G/3G/4G. It may be powered by batteries and power supply along with cradle for charging. • Capability to print real time parking receipts and QR-coded tickets • Transactions to be uploaded instantly and automatically to the POCC • Ticket dispensing & cash register functionality should be possible within a single device. • it should be possible to scan the QR Code on tickets issued by the entry device and issue receipts post payment • It should be possible to validate QR Codes for reserved or drive-in users using the Mobile Parking application MPOS Billing Application • The application should enable retrieval for transaction ID by at the least 3 methods to calculate the parking fee at exit or during any time vehicle is parked for security or other reporting reasons i.e. Scanning Paper QR Code, Entering Mobile ID, Entering Unique ID Printed on ticket • POS Application shall be Android Based • Application shall be capable to validate drive-in and reserved users by scanning QR Code generated on Mobile Parking Application of commuters • The POS software should be able to differentiate & handle between Normal Paid Parking users, VIPs and guests who are not supposed to pay parking charges • The POS software should be able to handle loss of entry ticket/pass • The POS application shall have an option to open boom barrier through handheld entry device • The POS application shall have an interface to enter car number, car type etc. parameters • The POS application, POS Portal, Parking guidance software, Parking Management Software, security enforcement software, live map view software, dashboarding, reporting and analytics software and user mobile Application may be an integrated suite developed by one company/OEM
	Boom Barrier
i.	High quality boom barriers have **10 million open/close cycles**
ii.	Comes along with induction loop for safety and security
iii.	No. of open/close data, loop trigger time etc. available for analytics and auditing.
iv.	The barrier booms should be optimized for use in parking applications: with the boom breakaway option
v.	Inter-ops with POS Entry device

vi.	Power consumption max. 95 W
vii.	Voltage 85–264 VAC, 50/60 Hz
viii.	Duty cycle 100%
ix.	Housing dimensions (W x D x H) 315 x 360 x 915 mm
x.	Enclosure rating IP54
xi.	Temperature range −30 to +55° C
xii.	Configurable open/close times of the barriers (0.9 sec, 1.5 sec or 3 secs etc.)
2.	Parking Guidance System
2.1	Outdoor Sensors
i.	Wireless Magnetic Sensors
ii.	Protection Level: IP67
iii.	Ability to accurately detect if the car bay is vacant/ occupied through appropriate placement within each bay.
iv.	Should use *magnetic sensors which can be safely fixed on road surface/ parking pavement*
v.	*The sensor should be interrupt based. Should not poll and check repeatedly for every few seconds if a vehicle has arrived/left.*
vi.	Sensor Shall reliably detect presence/ absence of car within a configurable number of seconds of car parking/ un-parking event occurrence
vii.	*The sensor should feature a selectable I2C or point-to-point SPI serial interface with 16-bit magnetometer ADC resolution along with smart-embedded functions*
viii.	*The transceiver should work in the open 2.4Ghz range*
ix.	*The transceiver should follow a mesh networking multi-hop protocol*
x.	*The sensor should have a fixed magnetic measurement range of ±1200 μT*
xi.	*The output data rates (ODR) from 1.563 Hz to 800 Hz are selectable*
xii.	*The sensor should be guaranteed to operate over the extended temperature range of –40 °C to +85 °C*
xiii.	*The sensor should send battery status at regular intervals*
xiv.	*The battery should have minimum life of 5 years*
xv.	Each sensor should have an accurate and real-time feedback mechanism to be detected automatically by the system in case of faults.
xvi.	Parking guidance software, floor map view software, digital display systems, outdoor sensors shall be from a single OEM.
2.3	Gateway routers
i.	Should be Linux based operating system powered gateway
ii.	Broadcom BCM2837 64bit ARMv7 Quad Core Processor powered Single Board Computer running at 1.2GHz Should have a 1GB RAM
iii.	The receiver on the gateway should use a 2.4GHz range and follow a multi hop mesh networking protocol
iv.	The gateway should periodically update the central management server at POCC about the diagnostics status of each sensor, LED, controller and display

v.	The gateway should use secure http protocol to communicate with the cloud server
vi.	The gateway should be able to control the displays placed throughout the parking lot
vii.	The gateway should ensure the display data sync at all locations and floors where they are placed
viii.	Should have Wi-fi on board, Ethernet connector on board
ix.	Should have Bluetooth Low Energy (BLE) on board for future tech integration
x.	Should have multiple USB ports for communication via USB GSM/3G/4G dongle
xi.	Should use micro SD port for loading your operating system and storing data
xii.	Should have a Micro USB power source (up to 2.4 Amps)
2.4	Digital Display Systems
i.	Should receive the data wirelessly
ii.	The displays should get the data within 5 seconds of change of status and the time limit should be configurable
iii.	LED matrix panel should be used to display the parking numbers
iv.	The text on the display should to be LED powered and 3-d projected
v.	The body of the display should be made of Aluminium Composite material (ACP) and be all-weather resistant
vi.	The displays should communicate the diagnostic data periodically with the gateways
vii.	The Digital display panels units should indicate available spaces for each parking slot/ bay /zone /level, total parking and the same should be controlled by the software
viii.	The display panel should be easy to understand and must have graphical directional and zone status indication (to guide drivers to zones with available spaces). The display panel shall be installed on each parking lot and on the approach roads/junctions to/within the parking lots so that commuter can check the availability of all parking bays ahead in advance and can take the suitable route based on parking availability.
2.5	Parking Guidance Software
i.	The guidance software should get real-time information of parking availability from the sensors
ii.	The guidance software should provide floor information if the parking lot is a multi-level parking lot
iii.	The guidance software should reflect change of status in the parking lot within 5 seconds and should be configurable
iv.	Real-time hardware diagnostics should be provided. Real-time data from sensors, LEDs, controllers, gateways and displays should be collected and displayed
v.	The diagnostic data should mention which sensor is working and which is not
vi.	The diagnostic data should also show live battery status of the sensors in real-time
vii.	The diagnostic data should mention which display monitors are operational and which are un-operational

viii.	Parking guidance software, live floor map view software, digital display systems, indoor & outdoor sensors shall be from a single OEM.
ix.	The individual slot/bay addition should reflect the total capacity and availability numbers
x.	The software should have the ability to disable specific parking bays and the same should reflect on the capacity and availability numbers
2.6	Parking Guidance Dashboards, Reports & Analytics
i.	Reports for Parking Guidance System should include (analytics for data collected from sensors on each slot)
ii.	▪ Slot level usage ▪ How many vehicle-rotations/slot for a day or any other custom period ▪ Average occupancy time of each vehicle on each slot ▪ Low slot usage information (if a slot is never being used, it will be shown on this report) ▪ High slot-usage information ▪ Peak-hour in-traffic ▪ Peak-hour out-traffic ▪ Occupancy hot-spots on the layout view ▪ Average turn-around time of each slot (on an average, how long does it take for a new vehicle to come into a parking slot, after a vehicle has exited that slot)
iii.	The reports and analytics should be downloadable on an excel sheet
3.	Parking Management Software Platform
3.1	Parking Management Software
i.	Parking management software should allow the operator to add/delete additional parking areas
ii.	Along with addition of parking lots, the software should allow the user to specify number of parking levels and total number of slots on each floor
iii.	Shall integrate multiple parking slots operated by a single operator
iv.	Shall integrate multiple parking slots operated by multiple parking contractors
v.	The software should allow adding individual slot specific information on each floor and map them to individual sensors
vi.	The parking management software can be used to add geographical location of the parking areas which should be reflected on the real-time parking information app to be provided to public
vii.	The software should allow parking slots to be configured as premium slots or non-premium slots
viii.	Parking slots should be allowed to be selectively enabled/disabled from the software
ix.	Manage online bookings for parking
x.	Manage monthly, quarterly, half-yearly and yearly passes
xi.	The software should enable payment and refund handling

xii.	The software should allow the user to set dynamic pricing for POS devices
xiii.	The software should allow a very robust minute-wise pricing scheme for the POS devices
xiv.	Open software architecture (API / Universal Interfaces)
xv.	Multi-tasking/multi-application capability allowing to open several operation modules at the same time
xvi.	The system shall generate alerts for over parked cars for security enforcement
xvii.	The POS application, POS Portal, Parking guidance software, Parking Management Software, security enforcement software, live map view software, dashboarding, reporting and analytics software and user mobile Application shall be an integrated suite developed by one company/OEM
xviii.	There shall be a provision that new entries to the car park are not permitted in case of the full occupancy of the Car Park
xix.	unique Identity for each transaction shall be created
xx.	Provision for user name and Passwords to restrict use to authorized persons only. Separate provisioning for Administrator and for General User
xxi.	Shift reports including Operator name, Shift number and Shift wise traffic & transaction details
xxii.	Daily & Monthly Summaries
xxiii.	Various reports for efficient management
3.2	Web Portal for Commuters
i.	The portal should have open APIs for 3rd party integration
ii.	The software portal should be developed with Angular JS platform
iii.	Portal must be omni channel i.e. its design should be such that it can be viewed easily on laptops, tablets and mobiles
iv.	Should be browser independent and work seamlessly on all leading browsers
v.	Should have workflow capabilities about the content approval and publishing process
vi.	Provisions to track and generate web traffic reports for Portal administrators
vii.	Citizen registration: • One-time online registration to be done and stored in the data center. • Terms of service to be accepted by the user prior to log-in
viii.	Parking Guidance System: • Current GPS location determined. • User enters destination • Nearest available parking spaces are shown using maps in decreasing order of distance, the rates of each parking applicable at that time shall also be displayed and if user decides to reserve it, reservation is done with payment done from e-wallet/ payment gateway

	• Number of vacant parking slots in a parking on map should also be shown to user.
ix.	Shall be browser independent and responsive to run in the same manner on leading browsers like Google Chrome, Mozilla Firefox, Safari, Internet Explorer, etc
x.	Shall support Unicode and be multilingual in at least English and Hindi.
xi.	Shall have provision for patches, hotfixes and bug fixing solutions.
xii.	Shall adhere to the best possible security standards in the industry.
xiii.	Shall support minimum Web 2.0 capabilities
3.3	Live floor-plan map view
i.	**MAP View software should provide slot-wise information**
ii.	**The software should clearly state which slot is occupied and which ones are unoccupied in real-time**
iii.	**Any change of status on the parking slot should be communicated to the software within 5 seconds and should be configurable**
iv.	**The entire parking lot's floor plan should be displayed on the software, either from CAD diagrams or manual mapping of slots within the parking lot**
v.	**The layout view should provide slot-wise live parking occupancy information**
vi.	**The layout should be easily designed and configurable based on any changes on the ground**
vii.	**The layout should be designed on a easily editable mark-up language such as scalable vector graphics (SVG) and should not be in any image format**
3.5	POS Portal
i.	The POS portal should provide live revenue collection data in real-time
ii.	The POS portal should provide a dashboard with 2-wheeler, 4-wheeler and booking's revenue collection information
iii.	The POS portal should provide filters for: a. Vehicle number search b. Vehicle type – 2w/4w c. VIPs (for whom parking fee was not charged) d. Guests (for whom parking fee was not charged) e. Time specific data retrieval f. Loss of pass transactions g. Entry operator search (from the operations side who gave the QR coded ticket) h. Exit cashier search (who collected cash for that transaction) i. Number of vehicles still inside the parking premises
iv.	Allow dynamic pricing for POS devices
v.	Allow minute-wise pricing
vi.	Allow provision for Do-Not-Count Minutes(DNC), where the software null's payment for those initial minutes

vii.	The POS application, POS Portal, Parking guidance software, Parking Management Software, security enforcement software, live map view software, dashboarding, reporting and analytics modules and user mobile Application shall be an integrated suite developed by one company/OEM
3.6	Dashboards, Reports & Analytics - POS
i.	The reports and analytics should be downloadable on an excel sheet
ii.	Reports for POS should include (analytics for data collected from the billing devices) ▪ Detailed report of daily, weekly , monthly and any other custom date range audit reports ▪ Revenue trends to be displayed in the form of bar charts ▪ Number of vehicles in/out with in-time and out-time ▪ Duration of stay of each vehicle ▪ Number of commuters along with the vehicle registration number ▪ Number of users that lost their passes and were charged a fine for the same ▪ Employee tracking ▪ Which employee was collecting cash and what was the actual collection for that day/period ▪ Average occupancy time of each vehicle ▪ Peak-hour in-traffic ▪ Peak-hour out-traffic
4.	User Mobile Application
i.	All applications, content, data, and information related to the App and users should be securely hosted and saved in the POCC
ii.	Free to download and use for all citizens, guests and visitors
iii.	Should be light, intuitive, easy to use, responsive, secure and maintain
iv.	Compatible with and responsive to all leading smart phones on Wi-Fi, GSM and CDMA networks V
v.	Operating System (OS) should be independent and available on all major OS platforms including iOS, Android, Windows
vi.	The parking application should be developed in native code
vii.	The application should be integrated with google maps to provide live parking data
viii.	The application should be integrated with payment gateways or mobile wallets for digital transactions
ix.	The application should provide the live floor-plan of the parking lot with parking availability on each slot
x.	The application should allow users to reserve parking slots and pre-pay for the same
xi.	The application should have provision for paperless transaction and allow the users to enter their vehicle registration number. Each vehicle registration number should be uniquely identified with a QR code. The application should be integrated with the POS system where the

	vehicle QR can be scanned at the entry to gain access to the parking lot
xii.	The application should also support geo-fencing
xiii.	The application should help commuters remember their parking slot after they have parked their cars
xiv.	The application should have in-app support system such as 24/7 live chat with customer support team
xv.	Citizen registration: • One-time online registration to be done and stored in the data center. • Terms of service to be accepted by the user prior to log-in
xvi.	Parking Guidance System: • Current GPS location determined. • User enters destination • Nearest available parking spaces are shown using maps in decreasing order of distance, the rates of each parking applicable at that time shall also be displayed and if user decides to reserve it, reservation is done with payment done from e-wallet/ payment gateway • Number of vacant parking slots in a parking on map should also be shown to user.
xvii.	Online cancellation for the spot should also be provided in case of online reservation.
xviii.	The App should integrate with and allow payments through the selected third part shared services for Payment Gateway and e-Wallet
xix.	The App should have a section detailing frequently Asked Questions (FAQs) related to Smart initiatives and their related responses. The section should also provide contact information of Helpdesk Customer Service for parking problems, if any
xx.	User should view version and details of the App
xxi.	Should be scalable and technically adaptable to future enhancements
xxii.	Should support Unicode and be multilingual in at least English and Hindi
xxiii.	Should track GPS location of the user device
xxiv.	Should provide accurate mapping and navigation services.
xxv.	Collect data categorically without impacting citizen’s privacy issues
xxvi.	POCC should provide live feed from parking lots and number of free spaces to app
xxvii.	Command Centre should confirm acceptance of payment and reserve/cancel the parking lots accordingly

5.1.5.7 Environmental Management System

5.1.5.7.1 Functional Requirement of EMS

#	**Description**
1.	Shall be ruggedized enough to be deployed in open air areas on streets and park
2.	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, noise quality, weather etc.
3.	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole.
4.	Environmental sensor station shall monitor following 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, PM2.5, and TSP) sensor ▪ Temperature sensor ▪ Relative Humidity sensor ▪ Wind Speed sensor ▪ Wind Direction sensor ▪ Rainfall sensor ▪ Barometric Pressure sensor; and ▪ • Noise sensor.
5.	Solution shall display trends of environmental parameters based on user specific time periods.
6.	Data shall be collected in a software platform that allows third party software applications to read that data.
7.	Solution shall display real time and historical data in chart and table views for dashboard view of the Client.
8.	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.
9.	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.
10.	
6.1	▪ It shall comprise of an Industrial PC running latest version OS and compatible software. ▪ Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AAQMS and MMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, ½ hr, 1 hr, 4 hr, 8, hr, 24 hr and so on. ▪ Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer. ▪ System shall be able to perform nested calculations vector averaging and rolling averages. ▪ It shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client. ▪ Data retrieval from CMS via USB and DVD shall be possible. ▪ Generation of reports for pollution load, wind rose etc.

#	Description
	▪ Alarm annunciation of analyzer/sensor in abnormal conditions.
7	
7.1	▪ The environment sensors shall be integrated with the command control system to capture and display/ provide feed. The data it collects is location-marked. ▪ Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making. ▪ Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions. ▪ Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis.

5.1.5.7.2 Technical Requirement of Environment Management Sensors

#	Description
1.	**Carbon Monoxide (CO) Sensor** ▪ CO sensor shall measure the carbon monoxide in ambient air ▪ Range of CO sensor shall be between 0 to 1000 PPM ▪ Resolution of CO sensor shall be 0.001 PPM or better ▪ Lower detectable limit of CO sensor shall be 0.040 PPM or better ▪ Precision of CO sensor shall be less than 3% of reading or better ▪ Linearity of CO sensor shall be less than 1% of full scale or better ▪ Response time of CO sensor shall be less than 60 seconds ▪ Operating temperature of CO sensor shall be 0°C to 60°C ▪ Operating pressure of CO sensor shall be ±10%.
2.	**Ozone (O3) Sensor** ▪ O3 Sensor shall measure the ozone in ambient air ▪ O3 Sensor shall have a range of at least 0-1000 PPB ▪ Resolution of O3 sensor shall be 0.001 PPM or better ▪ Lower detectable limit of O3 sensor shall be 0.001 PPM or better ▪ Precision of O3 sensor shall be less than 2% of reading or better ▪ Linearity of O3 sensor shall be less than 1% of full scale ▪ Response time of O3 sensor shall be less than 60 seconds ▪ Operating temperature of O3 sensor shall be 0°C to 60°C ▪ Operating pressure of O3 sensor shall be ±10%
3.	**Nitrogen Dioxide (NO2) Sensor** ▪ NO2 Sensor shall measure the Nitrogen dioxide in ambient air ▪ NO2 Sensor shall have a range of at least 0-10 PPM ▪ Resolution of NO2 sensor shall be 0.001 PPM or better ▪ Lower detectable limit of NO2 sensor shall be 0.001 PPM or better ▪ Precision of NO2 sensor shall be less than 3% of reading or better ▪ Linearity of NO2 sensor shall be less than 1% of full scale ▪ Response time of NO2 sensor shall be less than 60 seconds ▪ Operating temperature of NO2 sensor shall be 0°C to 60°C ▪ Operating pressure of NO2 sensor shall be ±10%
4.	**Sulfur Dioxide (SO2) Sensor** ▪ SO2 Sensor shall measure the Sulfur dioxide in ambient air

#	Description
	▪ SO2 Sensor shall have a range of at least 0-20 PPM ▪ Resolution of SO2 sensor shall be 0.001 PPM or better ▪ Lower detectable limit of SO2 sensor shall be 0.009 PPM or better ▪ Precision of SO2 sensor shall be less than 3% of reading or better ▪ Linearity of SO2 sensor shall be less than 1% of full scale ▪ Response time of SO2 sensor shall be less than 60 seconds ▪ Operating temperature of SO2 sensor shall be 0°C to 60°C ▪ Operating pressure of SO2 sensor shall be ±10%
5.	**Carbon Dioxide (CO2) Sensor** ▪ CO2 Sensor shall measure the carbon dioxide in ambient air ▪ CO2 Sensor shall have a range of at least 0-5000 PPM ▪ Resolution of CO2 sensor shall be 1 PPM or better ▪ Lower detectable limit of CO2 sensor shall be 10 PPM or better ▪ Precision of CO2 sensor shall be less than 3% of reading or better ▪ Linearity of CO2 sensor shall be less than 2% of full scale ▪ Response time of CO2 sensor shall be less than 60 seconds ▪ Operating temperature of CO2sensor shall be 0°C to 60°C ▪ Operating pressure of CO2 sensor shall be ±10%
6.	**Particulate Profile Sensor** ▪ Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air ▪ Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better ▪ Range of PM10 shall be 0 to 450 micro gms / cu.m or better ▪ Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3 ▪ Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading) ▪ Flow rate shall be 1.0 LPM or better ▪ Operating temperature of the sensor shall be 0°C to 60°C ▪ Operating pressure of the sensor shall be ±10%
7.	**Temperature Sensor** ▪ Temperature sensor shall have the capability to display temperature in °Celsius ▪ Temperature range shall be -10° to +80°C ▪ Sensor accuracy shall be ±0.3°C (±0.5°F) or better ▪ Update interval shall be 10 to 12 seconds
8.	**Relative Humidity Sensor** ▪ Range of relative humidity sensor shall be 1 to 100% RH ▪ Resolution and units of relative humidity sensor shall be 1% or better ▪ Accuracy of the sensor shall be ±2% or better ▪ Update interval shall be less than 60 seconds ▪ Drift shall be less than 0.25% per year
9.	**Wind Speed Sensor** ▪ Wind speed sensor shall have the capability of displaying wind speed in km/h or knots ▪ Range of sensor shall be 0-60 m/s ▪ Accuracy of wind speed sensor shall be ±5% or better ▪ Update interval shall be less than 60 seconds
10.	**Wind Direction Sensor** ▪ Range of the wind direction sensor shall be 0° to 360° ▪ Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display

#	Description
	▪ Accuracy shall be ±3% or better ▪ TR 6.70 Update interval shall be 2.5 to 3 seconds
11.	**Rainfall Sensor** ▪ Rainfall sensor shall the capability of displaying level of rainfall in inches and millimeter ▪ Daily Rainfall range shall be 0 to 99.99” (0 to 999.8 mm) ▪ Monthly/yearly/total rainfall range shall be 0 to 199” (0 to 6553 mm) ▪ Accuracy for rain rates shall be up to 4”/hr (100 mm/hr) or ±4% of total ▪ Update interval shall be less than 60 seconds ▪ 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
12.	**Barometric Pressure Sensor** ▪ Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa/mb ▪ Range of barometric pressure sensor shall be 540 hPa/mb to 1100 hPa/mb ▪ Elevation range of the barometric pressure sensor shall be -600 m to 4570 m ▪ Uncorrected reading accuracy shall be ±1.0 hPa/mb at room temperature or better ▪ Equation source of the sensor shall be Smithsonian Meteorological tables ▪ Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa/mb) or better ▪ Elevation accuracy shall be ±10’ (3m) to meet equation accuracy specification or better. ▪ Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa/mb) or better. ▪ TR 6.85 Update interval shall be less than 60 seconds
13.	**Noise Sensors** ▪ Noise sensor shall detect the intensity of the ambient sound in a particular area ▪ Nosie Sensors shall be installed for the outdoor applications ▪ Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA ▪ Noise sensor shall have resolution of 0.1 dBA
14.	Integration with ICCC solution, VMSB, Portal and Mobile applications
15.	Conditions-Ruggedized enough to be deployed in open air areas on streets and park

5.1.5.8 Web Portal and Mobile Application

Overview

At the core of the stakeholder’s service experience will be citizen portal of KSCL which will be a gateway to citizens, tourists and businesses for disseminating information and engagement. It will be accessed by citizens, investors and corporates alike and shall provide factual and attractive information to investors. The portal should clearly communicate a sense of ‘identity’ at first glance. The Portal will have an intuitive user interface for rendering various services and providing role based access to various systems in use. Through the Portal, any user can seek information, request for services, status check on service request, lodge an incident/complaint and provide suggestions. Portal shall exhibit enriched infographics on various parameters of smart solutions.

Portal should serve as a cutting-edge communication tool that clearly conveys its mission, vision, offerings and purpose. The site shall help prospects and citizens to better understand and engage with the KSCL's mission. Portal shall be a useful tool for the target audience, while being visually appealing, user-friendly, and state-of-the-art. It must allow easy navigation. Portal must have an attractive mix of text, images, audio and video.

The portal should:

- increase traffic and visitor engagement through architecture, design, and other features such as social media integration
- help visitors easily understand the corporation's mission and obtain information about KSCL's offerings
- deliver content concisely and clearly; includes dynamic information

The portal should have links to log-in for visitors (through APIs of Gmail/Facebook etc.) and employees. This log in shall redirect the user to the portal with rights to view or update content as per user status. The home page shall be clean and visually compelling that quickly conveys to the visitor, corporation's mission and what the KSCL does. This shall include dynamic 'Call-Outs' which highlight what's new on the website as well as information sliders. The portal should primarily be available in Hindi & English.

Mobile enablement framework will be deployed for KSCL, which deals with both rendering the portal in mobile devices through necessary UI components as well as making native mobile apps for mobile platforms i.e. Android, iOS, Windows. App shall be available on App store (iOS), Google play store (Android) etc. for freely downloadable for interested stakeholders.

Refer subsequent section for minimum functional and technical requirement specifications.

5.1.5.8.1 ERP

ERP provides an integrated and continuously updated view of core business processes using common databases maintained by a database management system. ERP systems track business resources—cash, raw materials, production capacity—and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data ERP facilitates information flow between all business functions and manages connections to outside stakeholders. Various features envisaged for the proposed ERP system in Authority, are being elaborated here:

5.1.5.8.1.1 Functional and Technical Requirements:

a. Architecture

- Centralized Server Architecture (n-tier architecture with web enabled user interface)
- The presentation logic should be decoupled from the business components logic

- Data access layer should be on RDBMS platform. Backend RDBMS should be of latest proven version of leading RDBMS.
- Single Database (No Heterogeneous Database to be allowed as part of the proposed solution.

b. User Interfaces

- The solution proposed should be Unicode compliant. Authority envisages requirements for both English and regional language for Data Entry, Display, Input and Output
- Single Sign-on (for all the users) for accessing all the modules
- Any data entry needs to be carried out only once and further it should be made available as often as necessary to all the systems by providing pre-fill feature
- All modules should be homogeneous with respect to Keyboard use, screen layout and menu operations with Graphic User Interface (GUI) support
- GUI Form Administration should support
- Changing fields or tab labels
- Hiding fields or tabs.
- Changing the position or size of field or labels
- Adding restrictions like mandatory or not
- Setting default value in a field
- Changing list of value (LOV) contents
- Capability to setup logic to trap conditions to pop messages in response to conditions like logical data entry errors, certain conditions etc.
- Ability to provide various configurable parameters down to the end user level so that the user screens can have different functionality for a given user.
- Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

c. Access & Data Security

- Role based authentication for accessing various functionalities of different modules with encrypted passwords. Access Rights can be given to Individual Users or Groups
- Flexibility to define separate Role and Designation to the users. Upon transfers of officers / employees, applications / letters / complaints pending with the employee shall remain to the role and new employee will be able to take action on these applications / letters / complaints.
- User rights to various forms should be Create New Record, View existing Record or

- Edit existing record.
- System should be able to capture exceptions to detect frauds / mistakes
- An audit trail of changes to data in the system should be maintained to identify the users responsible for the modification. There should be a facility to create reports on audit logs
-

Following minimum functional requirements are been envisioned in the ERP implementation:

-
- User – self registration and first time password change prompt.
- System would allow user to login and avail services from any of the modules.
- System would allow user to view any Service information from Departments displayed on Web portal.
- During user id creation system would ask for Security question for any password reset request by user in future.
- System would prompt user to create password as per security policy.
- Alphanumeric passwords would be asked.
- System would ask user to create a transaction password to be used for performing any financial transaction with the concerned departments or while making any changes in the profile.
- During user id creation, system would ask user to furnish all personal details like

Name

Gender

Age

Address

Phone no.

Email id

Occupation

Family details

PAN/License/Passport/Voter Registration No./UID No. or any other Id proof details.

- System would prompt user to login using user id and password created and verify them.
- On successful password match, system would allow the user to login to the portal and allow him to access his/her profile. On unsuccessful password match,

System would generate password error message and ask user to enter correct password in order to login to his/her profile.

- System would allow user to edit his/her personal details like Name, Address etc.

- System would display the service related information/Instructions to fill up requested details in the entry forms like applicable fee and documents to be attached/submitted along with application request.

- For CCC Operator, system would initially allow CCC operators to login using their login ids and passwords as given by System administrator. After first time login by all CCC operators the system would ask them to change their password (alphanumeric) as per the security policy.

- After successfully changing the password and verifying the same on to the system, CCC operator would get access to all the modules, can accept and insert details of the requests received by the citizens for specific modules.

- System would display instructions to CCC operators at the time of inserting details in the request form for various applications.

For the design and development of intranet portal for the Authority for having exclusive access to employees of the Authority, same rules of user creation and authentication may be followed in addition to provisioning of device MAC no. being used by the official and also the domain in which the user is accessing the system. Messages and alerts would also be required to be provided on mobile and other user interfaces. It will also have system administration module for creation of user ids for various roles and responsibilities as per the official levels of officials for access to various privileges. Important applications in the intranet portal would be

- Employees Information System having unique Employee ID
- Payroll Package
- Leave Monitoring System
- Biometric based Attendance System
- Employee Performance Monitoring System, etc.

A. Profile Management:

Enable registered users to manage their accounts and profiles and as appropriate

B. Security

Based on ISO 27001/BS 7799 standards, user access to the system must be through a single sign on process, which should involve specification of a user

Identification, a password and the applications displayed must be as per the user profile and authority. The system should al low user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the User profile after five unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system. This section highlights the security architecture proposed for the e-Municipality system:

I. General Requirements

i. Information, hardware and software would be secured to both internal and external parties (such as through password encryption).

ii. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.

iii. System level and application level authentication between portal and between

- applications within portal, if any, to ensure against security attacks

vii. There should be four levels of security considerations as described below:

a. Key Security Considerations at the User level:

(i) User authentication

(ii) Role based access to services, transactions and data

b. Key Security Considerations at the Network/ Transport level:

(i) Network Link Encryption (IPSEC)

(ii) Encrypted HTTP session using SSL (HTTPS)

c. Key Security Consideration at the Infrastructure Level:

(i) Firewall to filter unauthorized sessions/traffic

(ii) Intrusion Prevention System to detect/ prevent unauthorized activities and

sessions

d. Key Security Considerations at the Application & Database level:

(i) Secure storage of user credentials

(ii) Server–to-Server communication encryption

(iii) Secured/ encrypted storage of data/ data elements in the Database & DB Backups

(iv) Comprehensive logging & audit trail of sessions and transactions

Unified Messaging system:

SMS: The Web-Portal shall have facility to send SMS to Mobile number of a citizen which was provided while requesting certain information or service. The SMS shall be auto-generated based on the information or service requested on occurrence of its change of status. All the application needs to be integrated with SMS gateway.

E-mail: The Web-Portal shall have facility to send e-mails to

- The e-mail address of a citizen, provided while requesting certain information or service.

- The e-mail shall be auto-generated based on the information or service requested on occurrence of its change of status.

- Reporting Officials maintaining the hierarchy, in cases of delay (as per the Citizens' Charter) in providing services.

Workflow Management System:

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of the service delivery channels. Each request/application should be processed via workflow engine mechanism. I.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

A] Citizen Service Module:

- Citizen Help Desk
- Facility to lodge New Complaints, Check Status
- Facility to check citizen data, Bill Dues, Application Status,
- Payment Status, Renewal Status, Certificates issuance
- Inter & Intranet
- Citizen Charter MSC, Authority

B] Application Acceptance & Delivery of Outputs

- Department-wise categorization
- Allow system to accept service specific inputs
- Capture of Mobile No. of Applicant
- Re-submission of rejected application after compliance
- Check-list for documents to be submitted along-with application
- Define citizen charter (list of the officers & duration for service delivery) Authority

- Fees to be accepted Accounts
- Generate Token of Application acceptance
- Rejection Note in case of inadequate application
- Delivery of the output through CCC / Internet / KIOSK
- SMS alert to applicant upon decision SMS Gateway

C] Payment Acceptance

- Property Tax
- Accounts,
- Departmental
- Modules,
- Property Tax
- Water Tax
- Professional Tax
- Vehicle Tax
- License
- All Departmental Services
- Tender Document Fees
- Any other

D] Citizen Services (General) [Such services won’t have any department specific functionality. CCC module, by using Workflow Management System should be able to deliver these services]

- Marriage Certificate
- NOCs for other govt. departments
- Booking of various Corporation premises such as Halls,
- Community Halls, Open air theatre, Amphitheatre, Auditorium,
- Ground, Party Plot, etc.,
- Issue of health license for shop having area
- Any other services

E] Marriage Registration Sub-Module

- Design of Forms & Database for the Marriage Registration
- Functionality
- Capture of Thumb Impressions of the Applicants & Witnesses

- Capture of the Photograph of the Applicants & Witnesses
- Scrutiny of the Applications

F] Professional Tax

- Enrolment and Registry Enrolment of firms. (PEC & PRC) Property Tax,
- GIS
- Details of firms along with their contact details, address, etc. Property Tax,
- GIS
- Outstanding Professional Tax details for different firms. Property Tax,
- GIS
- G] Vehicle Tax
- Capturing Vehicle details such as Engine No/ Chassis no,
- Capturing type of Vehicle for collection of taxes.
- Capturing details of the Vehicle owner (Name, Address,
- Contact details, etc.)

H] MIS

- SMS alert to applicant upon decision
- Services Statistics, CCC / KIOSK, Department-wise
- Officer-wise list of services pending HRMS, WMS
- Marriage Registration periodic / statistical reports
- Professional Tax collection / outstanding report
- Interest calculation for outstanding Professional tax
- Defaulter list for Professional Tax payment GIS
- Property Tax collection report
- Report containing license issued details and payment
- collected for the same.
- Vehicle Tax collection report

I] Additional Functional Scope after validation

- RTI
- Issuing License : Gumasta License, Hawker’s License, Health license etc

These are the module to be the part of ERP system to provide service delivery the system will be flexible to scale up and configure the solutions and modules as and when required based on city requirement for governance and service delivery.

5.1.5.8.2 Web Portal

5.1.5.8.2.1 Functional and Technical Requirements of Web Portal

#	Description
1.	**Home Page** A clean, visually compelling home page that quickly conveys to the visitor, the KSCL's mission and what KSCL does. It will include (but not limited to) the following information either directly or linked through other pages: ▪ About KSCL; Corporation, Message from the CMD, Board of Directors, Shareholding pattern, Organogram & Key Personnel ▪ City Profile ▪ Master Plan ▪ Investment opportunities ▪ Key statistics ▪ Tourist Locations ▪ GIS map of the City ▪ Photo Gallery ▪ Online Services listing (e-governance services) ▪ Opportunities; Tenders, Careers, Empanelment, Training ▪ Downloads ▪ Links to Facebook, twitter etc. ▪ FAQs ▪ Feedback ▪ Contact Us ▪ Search ▪ News & Updates ▪ Log in ▪ Privacy Policy, Disclaimer, Visitors count, Important links, Site map
2.	**Branding:** Clearly communicates a sense of 'identity' at first glance.
3.	**Visual appeal:** The site must have an attractive mix of text, images, audio and video.
4.	**Fast Loading Pages:** Optimization of web pages for a faster browsing experience with compatibility with key industry browsers and platforms.
5.	**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 and adjust resolution and format accordingly.
6.	**Bilingual** The portal shall be available in Hindi & English and Unicode complaint.
7.	**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.
8.	**Search Tools:** Provide search capabilities using key words or phrasing that will provide access to content from throughout the site. Additionally, make it possible

#	Description
	to download historical and recent data whereby the user can define his/her preference. Platform should allow users to search content of the portal easily and quickly without the need of high speed bandwidth.
9.	**Important Links:** Links should be placed within the portal to allow individuals to contact institutions affiliated with the KSCL and access to the portal as well the respective departments/agencies/corporations/ministries.
10	**Easy access to Key performance indicators (Infographics):** Seamless presentation of dashboard data to provide continuously updated graphs and charts.
11	**News/Update feed:** Constant and dynamic update feed on portal home page. Displays announcements and notifications for new content additions on front page of portal.
12	**Calendar and bookings:** A dynamic calendar that displays events as well as filters for searching events and booking any available venues/functions.
13	**Contact Form:** Provides a web-based contact form with anti-spam controls and shall allow stakeholders to track the status of request at any point of time, if any.
14	**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.
15	**Social Media Engagement Tools:** New tools to improve interaction with social media.
16	**Search Engine Optimization (SEO):** Portal availability using common search engines to ensure it is optimized using SEO.
17	**Search capability:** Portal should provide search engine with advanced full-text search capabilities.
18	**Compatibility:** Site must be compatible with common operating platforms including Google Chrome, Microsoft® Internet Explorer 8.0 or higher, Microsoft Edge, Mozilla Firefox, and Safari 5.0 or higher.
19	**Mobile Access**: Portal must be "responsively designed" to accommodate mobile users. This also includes accommodations for slower, cellular internet connections. This includes compatibility with iOS, Android and other industry standard platforms.
20	**Settings:** Portal must not require plug-ins as a default.
21	**Performance:** Portal must be able to handle multimedia (video) with high performance.
22	**HTML Compliance:** Full compliance with HTML 5.0 or higher.
23	**GIS:** web GIS view of Kanpur Smart City depicting information through various layers would be shown to stakeholders; showing occupied and vacant land parcels, access to information on industries, residential properties, education & health facilities, transportation etc.
24	**Security:** Portal shall be secure against hacking and other vulnerable activities.
25	**Content Management System:** ✓ shall have Content Management System to update the content on the Portal which shall have minimum following capabilities: ▪ Content Authoring ▪ Content Publishing ▪ Content Delivery ▪ Content Storage Management ▪ Content Archival ✓ Separation of content from presentation, which allows authors to focus on content rather than web design.

#	Description
	✓ Content storage management of all types of content; text graphic, audio, video etc.
26	**Integration with other applications:** Different existing and future applications/modules shall have to be seamlessly integrated with the portal. It is envisaged that GIS and the proposed systems shall work in an integrated manner to allow KSCL to extract maximum benefits from the system.
27	**Design and Construction** ▪ Work closely with the KSCL 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 KSCL and standards for content management ▪ Platform should allow easy integration of multimedia products and user-friendly administrator interface ▪ Create wireframes, storyboards and prototypes to propose options for implementation. Provide five (5) template designs for review to select a concept ▪ Concepts should reflect the KSCL's identity, nature and purpose ▪ 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 portal ▪ Submit the final concept to KSCL for review prior to 'going live' ▪ Secure the existing portal prior to transitioning to the new platform ▪ Keep a full backup of the portal through the currency of the Project ▪ Manage all upgrades and updates on the website including content update in an efficient and integrated manner ▪ Portal design shall support easy upgrades and updates on content without the need to redo the base design.

5.1.5.8.3 Mobile App

With rapidly increasing levels of mobile penetration and continuous improvement in bandwidth, and requirements of accessibility and citizen convenience, it has been envisaged to offer information dissemination to stakeholders over mobile devices. There shall be a strong interfaces, technologies, applications etc. for mobile devices. In order to maximize citizen convenience and bring about business process improvements, the successful MSI shall continuously innovate, upgrade and incorporate such new technologies that emerge new avenues.

5.1.5.8.3.1 Functional and Technical Requirements of Mobile App

#	Description
1	Mobile app should mirror the portal and be adapted for optimum viewing on multiple operating systems and device sizes. However the actual application layout design for both mobile and web is the responsibility of MSI.
2	Mobile app must be based on latest HTML 5 and above.
3	Mobile app shall be native on Android, iOS and Windows platform.
4	Mobile app should be in Hindi & English.
5	Mobile app should be capable of showcasing enriched infographics to its stakeholders.

#	Description
6	Mobile app shall be designed in such a manner that it shall address the following key issues: ▪ Caching: Caching unnecessary data on a device that has limited resources ▪ Communication: Failing to protect sensitive data over any carrier ▪ Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity
7	Mobile app shall be integrated with main core solution proposed. There shall be facility to PUSH through and PULL through mechanism to get and receive information using SMS service.
8	Mobile app shall provide critical data such as user identification and location information including latitude, longitude and altitude.
9	The mobile app shall have the ability to take and transmit, pictures and videos in real time along with geo-tags from the device.
10	Mobile app should have capability of - ▪ Image compression, B/w conversion from color images ▪ Auto cropping, Auto orientation, perspective correction, geo capture ▪ Image capture setting (camera resolution, image type)
11	Mobile app shall have the ability to push information to the mobile app as well as post bulletins and resources on the mobile app through API's.
12	Platform will provide a report generating tool, which can be used to generate customized reports at any level.
13	Platform should allow for a graphical interface to view the summary data in MIS reports. This would include trend graphs, graphs indicating how much of the target has been met etc.

5.1.5.9 Enterprise GIS

Overview:

Availability of timely and relevant information about cityscape, the physical growth trend taking place in different parts of the city is a very important input to the Smart City Development process. Geographical Information System (GIS) is for management, analysing and displaying data of all areas within Kanpur Smart city which are spatially referenced to earth for efficient and effective decision making, spatial planning, management of crisis/disasters and for monitoring of normal circumstances, thus providing an important tool to respond faster to incidents or even avert certain incidents. GIS platform is intended to provide common GIS capability to all other systems being deployed as part of Kanpur Smart City initiative. The objective of architecting a common GIS layer is to keep a single repository of all GIS data (pan city data) for easy maintenance, avoid duplication and easy dissemination of information to all the dependent systems. The dependent systems include Smart Parking, City Wi-Fi, Pan City Network Backbone, Intelligent Transport Management and Utility Management Systems. More systems may be added in the future and therefore the GIS application should be able to integrate with such applications through standards based interfaces. GIS platform would be importing a lot of existing data from various sources into most industry standard formats. GIS platform would also need to exchange data with a number of external applications and therefore should be capable of exporting data in most industry standard formats Following services shall be configured through Web GIS software (but not limited to):

- Location Based Services
- Traffic Management System, Vehicle Tracking and Management System (VTMS)
- Mobile GIS Services
- “What if” analysis
- Mapping Gallery for Inter-Departmental use of Maps/ data Integration of Applications and disparate databases

Refer subsequent section for minimum functional and technical requirement specifications.

5.1.5.9.1 Functional and Technical Requirements of Enterprise GIS

GIS Base map Preparation

KSCL shall provide available GIS administrative data along with property layer to the selected MSI

MSI shall asses the quality of available GIS data and accordingly shall create the GIS data creation plan for remaining data layers in consultation with the KSCL.

GIS base map shall be a common platform across all the solutions including City Wi-Fi, Video Surveillance, Smart Lighting, Intelligent Traffic, Smart Parking, ICT based solid waste management, Intelligent transport, Disaster management, Incident Management & any other ICT component in consultation with KSCL.

MSI shall develop GIS based Decision Support System for public safety & law enforcement.

MSI shall use spatial & non-spatial information from GIS database to develop real-time management of various surveillance systems like Traffic Management, VTMS, Smart Parking and incident management, etc.

GIS database shall be in any OGC format;

GIS base map shall include following, but not limited these data with attributes with necessary attributes which shall be finalized during study phase;

a) Road Network

b) Railway Network

c) Administrative boundaries (KSCL Boundary, Ward Boundary etc.)

d) Building footprints and names

e) Points of Interest data includes:

□ 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 etc.)

□ 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 etc.

□ Local landmarks with locally known names.

f) Land-Cover (Green areas, Open Areas, Water bodies)

g) Address layers (Pin code, Locality, Sub-locality etc.)

h) Utility Networks (OFC, Water, Sewer, Drainage etc.

i) Locations of other Municipal Assets

j) Education (Primary/Secondary/High School/Colleges)

k) Religious structures

l) Community centres

Web GIS Decision Support System

User Creation and Security Management

Map Browsing Module

Data Editing & Search Module

□ Point

□ Line

□ Polygon

Data Analysis Module

□ Buffer

□ Spatial Overlay

□ Application Interface

□ Big Data support

Citizen Location Services

Generating Reports

Help File Creation

Thematic Mapping (On the fly)

User Creation and Security Management

Shall facilitate to create, delete & modify different Enterprise GIS Users within KSCL.

□ 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
- Maintain Interface with KSCL Internal Departments to resolve technical issues
- 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
- Shall not require opening of any special protocols for connecting the user client to the web/application server used by the package. All communication shall be on HTTP or HTTPs.
- 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.
- Application users shall not have direct access to the database.
- 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.
- Shall be possible to audit users at the form level, user level, application module level and at the organizational role level.
- Shall provide reports on user activity based on the role and the application that was used.
- Shall support configurable password policies including;
- Password expiry
- Password complexity
- Password history and reuse policy
- Forced password change on first log on
- Capability of self-service reset of passwords in case of forgotten passwords or locked accounts.
- Shall support security system with a full-fledged Role Based Access Control (RBAC) model

Map Browsing

This module shall mainly comprise of the basic map navigation tools and the most essential tools for identification of features and attributes. Following are some of the map browsing functionalities :

- Zoom in: The user shall be able to select a particular portion of the map by drawing a rectangle on the map specifying the extent into which the map shall be zoomed in to see the features more closely and in more detail.
- Zoom out: The user shall be able to select a particular portion of the map by drawing a rectangle or just clicking on the map to see the map at a smaller scale.
- Full view (Full Extent): The user can view the map in full extent after zooming in or zooming out at different scales

- Pan: The user shall be given an option to pan the map, which shall be possible if the entire map is not fitting into the screen, i.e., after the user has zoomed in to the map at a certain extent.

- Identify: The user shall be able to view attribute information of the feature of interest.

- Find: User can key in the desired area and the application shall highlight the area on the map.

- Measure distance/area: Two options shall be provided to the user. The user shall be able to measure the area and to measure the distance

- Refresh Map: All the selected features of the active map layer shall be cleared of the selection, by using this tool.

- Select Feature: User shall be able to select the features of active map layer

- Clear selection: User shall be able to clear selection that is there on map

- Activity indicator: Display notification while map/ data is being processed

- Scale input box: allow user to enter representative fraction scale for dynamic services - For cached services, scale box should contain dropdown menu of available cache scales (levels of detail)

- Show/hide co-ordinates: Show/hide mouse coordinates

- Print: The map can be printed in its current extent as viewed in the map window. The user would be presented with a layout for printing

- Descriptive Map Information Tool: When the mouse cursor hovers over each map feature, information should be shown based on the feature's attributes. Functionality should be available for all feature classes; should be able to display a combination of attributes and should not limit the number of features that can be included with the map tool. It should allow user to turn on and off as needed.

Data Editing & Search

- Shall provide the data editing capabilities including new data addition and existing data updation for geographical features and its attributes.

- Shall provide user to edit GIS Features. However, for a bulk data editing, KSCL shall use Desktop GIS facility, since web based data editing of large database may cause data corruption. Following are the steps for editing any features through Web GIS-

- Add Features

- Delete Features

- Move Features

- Modify Features

- Select Feature to Edit

- Feature Locate by Manual Browsing

- Feature Locate by Entering Lat and Long

- Feature Location by search criteria.

- Identify Feature to Edit

- Shall allow users to search features by both pre-configured and dynamic based on unique values as follows;
- Search by Ward,
- Search by area,
- Search by Plot/ CTS Number,
- Search by Building Number,
- Search by Sector,
- Search by UPID, Aadhar etc.
- Search by area,
- Search by Plot/ CTS Number,
- Search by Building Number,
- Search by Sector
- Search by Parcel ID etc.
- Shall allow user to run the custom queries on-the-fly and save those queries for shared future use
- Shall allow user to run spatial query on multiple layers with spatial operators
- Shall also allow for a buffer to be applied to the search criteria allowing for features within a certain distance of the query feature to be selected.
- Shall have facility to run combination of attribute & spatial query
- Shall have facility to auto-complete text boxes based on either feature attributes or linked records

Date Analysis Module

Shall comprise of analytical tools such as spatial overlay, buffer analysis to generate results, and shall also provide geo-processing functions that will be finalized at the time of study stage.

Visualization of Temporal Data

Shall have facility to visualize time aware layers

Shall allow user to add temporal data layer on-the-fly

Printing

- Shall have ability to print maps to a printer/plotter with the selection of paper size (A2, A1, A0, Letter, Tabloid etc.) and page orientation (landscape or portrait)
- Shall have print preview option
- Shall be able to handle and process any redlining / markups of the map.
- Shall have ability to export the map to a standard image format (BMP, TIF, JPEG and PDF file)

□ Shall have a variety of templates must be available which allow the user to add a custom map title and to decide which map elements (north arrow, scale bar, overview map, legend, etc.) will be visible.

□ Print date and time shall be automatically added to output at application runtime

□ Legend shall be automatically adjusted based layers displayed in print area

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 must 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.

Add Map Layers

Shall allow user to add GIS map layers

Added new map layer shall be overlaid on the existing map

Hyperlinks

Shall have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute

Emailing

Shall allow user to Email map as an attachment

Reporting

□ Shall provide predefined report templates

□ Shall allow user to create custom reports using SQL query interface and save those reports for shared future use

□ Shall allow user to generate reports on selected features

□ Shall be able track the history of reports a user has performed.

□ Shall be able to export reports into PDF and MS Excel

□ Shall allow use to select different date ranges to view report information

□ Shall allow user to print reports

Web-Editing

□ Support role based multi-user editing access and editing work flows.

□ Shall allow authenticated user to validate spatial feature create/delete/edit/upload through Web-GIS application

□ Shall allow administrator to Accept/Reject the changes made and a log shall be created for the same.

□ Shall have easy-to-use map editing tools

□ Shall allow user to divide the polygon or polyline

- Shall allow user to amalgamate the two or multiple polygons or polylines
- Shall allow administrator to configure the edit/view security at the level of feature attribute

Select Feature

- Should be able to select features by clicking on or by drawing a polygon around the feature
- Should allow user to generate URL for current view extents, visible layers, and active selection
- Should allow user to email the generated URL
- Should allow user to export data into KML/KMZ and Shapefile

Bookmarks:

- User should be able to save a map view and be able to return to that exact view at a later date
- User should have ability to email the current view extents, visible layers, and active selection in the form of image

Application Error Reporting:

Should allow user to report errors, with a screen capture, back to the KSCL GIS Coordinator

Technical Specifications

Layer and data security – it shall have a provision to configure user level access to data and layers.

Shall be compatible for accessibility from any device (i.e. Mobile, Tablet and Laptop), Standard Operating Systems and Internet Browsers.

Shall support One-Web functionality

Shall have provision for flow of information and/or integration with existing and future applications (indicative) such as:

- Smart Lighting,
- Vehicle Tracking System
- ICT based solid waste management
- Intelligent Traffic Management System
- Intelligent Transport Management System
- Smart Parking Management System
- Environmental Sensors
- Wi-Fi Hotspots
- Smart Water Supply Management
- Property Tax management system
- Building Plan Approval System
- Enterprise Project Management

- Any other Municipal e-Governance Application

It shall be a single window application to visualize MIS and GIS data on the same platform.

It shall be have User Management component for defining user roles to control the access of tools and database as per KSCL's requirement.

It shall have a provision to perform Quality Control activity on the data collected from the field before storing on the parent database server.

It shall have provision to generate custom reports.

It shall have provision to generate thematic maps on-the-fly based on attributes details available in the GIS layers

It shall have a provision to store audit trail of user activities performed on the application.

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.

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.

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.

Shall be able to toggle between Web-GIS and external applications.

Shall allow user to view the maps and attribute data (in limited form) from external applications as well as from the Web GIS window and perform basic functionalities of external applications through the web-GIS window and vice-versa.

Shall be supported with Internet Explorer 9 and above, Latest version of Chrome, Mozilla & Safari browser etc.

System is expected to realign and fit to the smart mobile devices (iOS, Android etc.).

Solution should be compatible with various open standards and technologies and should not restrict KSCL in using the solution data for any other applications, and should compliance National Data Sharing and Accessibility Policy (NDSAP) dated 17 March 2012, India's open Government data guidelines.

Standardization and Interoperability – the proposed Web GIS Map engine shall be OGC (Open Geospatial Consortium) and SWE (Sensor Web Enablement) compliant.

Distance and Area Measurement

Should have distance measurements tool to allow user to measure the length of irregular shaped lines

Should have area measurements tool to allow user to measure irregular shaped polygons

Measurements should be shown using the metric and the imperial system. The ability to snap to the edge or nodes of the feature being measured is desirable

Event based trigger

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.

Hyperlink

Should have ability to hyperlink to document, images, avi files and PDF files with the feature's attribute

Dashboard

Should provide easy-to-understand, easy-to-use reports that use appropriate infographics (Charts) to present key indicators from the GIS database, to provide overall information to the key officials

Should have a GIS-enabled real-time dashboard to display dynamic charts & graphs

Video / CCTV Surveillance Interface

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

Web portal capability:

Facility for display of spatial layers, query management like have various query tools for queries based on attributes, location, etc.

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.

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

5.1.5.10 City Wi-Fi

5.1.5.10.1 Overview:

Hot Spot Wi-Fi serves as the foundation for creating a connected city to access the wireless internet service with ease and convenience. For this purpose KSCL has identified locations where these services has to be provided to citizens. As a part of this initiative free Wi-Fi need to be provided; Wi-Fi shall be free for the first 30 Minutes per Mobile subscriber per day with aggregate limit of 5 GB per month whichever is achieved first beyond that it is chargeable. Beyond the above specified limit services would be chargeable by KSCL. For implementing the same the Bidder will carry out survey at these 86 locations (tentative) and will deploy the access points as required for providing the Wi-Fi services. As a part of Wi-Fi solution the MSI needs to provide Wi-Fi controller, DNS, Internet bandwidth from Internet Service Provider (ISP). ISSID for E governance (for Client) shall be reserved. For installation of Access Points, if there is any requirement of additional poles, the same will be provided by Bidder at its own cost with prior approval from KSCL

City Wi-Fi Hot Spot helps cities provide citizens with Internet connectivity and access to a broad range of citywide service which has following benefits:

- Internet availability at lower costs
- E-government services delivered to citizens, faster, and at a lower operating expense
- Local economic development
- Improved productivity and service
- Access to city services and Internet connectivity
- Increased access to online services
- Revenue generation

MSI shall be responsible for establishment of Wi-Fi network at the selected location in the KSCL, these locations are normally tourist spots, public places or any other identified place by KSCL. MSI shall provide Operation & Maintenance throughout the contract period from the date of commissioning. The broad scope of work for MSI during the entire project period would be as under;

MSI Shall undertake a Site-survey of all the specified sites and submit a site wise survey report to KSCL mentioning the location &number of Access Points (APs) required to be installed at each site.

MSI proposal must provide all the necessary electronic components needed to provide wireless access to the public. This includes but is not limited to Wireless controllers, Access points, Power over Ethernet devices, L2 and L3 managed switches, Routers, UPS, passive components i.e. UTP, OFC, Electric wires, racks etc.

MSI shall install the Access Points at approved locations (on directions by KSCL after approval of Site-Survey report). The power points, connectivity and LAN points will be the responsibility of Bidder. KSCL will facilitate the requirement/clearances as and when required.

MSI shall properly Wall Mount/ Pole Mount the Access Points at approved locations with external mounting kit as per OEM standard practice.

MSI shall install the AP Controller, NMS, NAS and required software at Command & Control Centre

The Patch Cords, Power adapter, Power cables, connectors, mounting kit and other required accessories for successful commissioning of the Wi-Fi network shall be provided by the MSI and shall be properly cased and tied such that it doesn't get broken.

Each controller should be ready for supporting 300 AP's and 20000 devices from day one to run in Active-Standby / Active-Active Load Balancing Mode, with scalability for 1000 AP support in future.

Each wireless device (not system) must support per SSID traffic shaping and limiting at line- rate at the Access Point (not controller). This is to prevent additional data on the network

Each wireless device (AP) must employ a future-proof modular architecture for upgradability to future standards

Bidder must include PoE-injectors in the pricing and clearly define where PoE injectors are needed

System must include a centralized management system that provides a platform for central management of all devices across the network

PVC case wiring should be done for the entire required passive cabling i.e. UTP and electrical wiring

MSI will ensure a secure Wi-Fi connectivity and internet access through user Login ID and password to all the subscribers with central authentication mechanism

MSI shall ensure that unique user ID and Password do not have provisions for simultaneous multiple logins

Policy on validity of the user ID and Password for internet access should be configurable as per the requirement.

Wi-Fi access points (APs) must be configured to use cryptographic keys or other methods to ensure that only authenticated users can use the Wi-Fi services

Internal / External AAA server should be deployed ensuring DOT guidelines for providing public Wi-Fi access. The log trails for any specific user shall be made available online for at least last 3 months and the backup shall be kept for one year.

The system should be capable of managing automatically upgrade or degrade of end-user's account after threshold usage (download/time limit) is reached

Wi-Fi network should be secure and conform to the industry standard security requirement. Bidder shall suggest and help KSCL team to deploy policies at various levels (i.e. on firewall, IDS, antivirus etc.) to prevent any attack/intrusion in the Wi-Fi network

MSI shall be responsible for integrating the Wi-Fi Network with the existing LAN/SWAN network

MSI shall be responsible for integrating the available payment gateway(s) at KSCL for making online payments (if any) according to respective plans for internet usage

MSI shall be responsible for integrating SMS gateway (HTTP) at KSCL for automatically sending the required details/ information through SMS to the users as per the requirement e.g. during user registration, forgot password, password reset etc.

5.1.5.10.2 Scope of Work:

5.1.5.10.2.1Functional and Technical Requirements:

5.1.5.10.2.1.1 Technical Specifications - Centralized Wi-Fi Management System

#	**Minimum specification**
1.	KSCL proposes to procure a centralized authentication system for its proposed Wi-Fi network. The system shall authenticate the City WiFi users of KSCL. The system shall also provide facilities like web self-care.
2.	The system shall comply to the DoT guidelines regarding provision of Wi-Fi internet service under un-licensed frequency band
3.	The Solution Shall Support Captive portal having customizable GUI. This portal should be available to any client coming into the Wi-Fi zone of KSCL
4.	Captive portal shall allow local branding and content as per the location.
5.	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
6.	The solution shall support Usage based as well as Time duration based accounting. It shall support real time disconnection on completion of allotted resources i.e. Time or Data
7.	The solution shall support centralized server for User authentication
8.	The application should be IPv4 and IPv6 compliant.
9.	GUI based management console for system administration, policy / package creation, backup and restore accounting data, SMS gateway configuration etc.,
10.	Tool for Troubleshooting and Health Diagnostic
11.	Creation of batches in advance and activation upon first usage
12.	Generation of report of usage and accounting, real time usage of USER as per the location.
13.	Access Control List for different accounting and report related activities
14.	Management of different Packages.
15.	Centralized system shall available in Failover mode
16.	Policy based access control for administrative activities

#	**Minimum specification**
17.	Login and session details, browsing history and audit trails
18.	Creation of subscribers as per the required packages. Activation of subscribers as per the usage
19.	Renewal / Registration of the subscriber.
20.	Portal providing Self registration.
21.	Creation of various packages
22.	Real time accounting of the usage
23.	Location wise usage and billing detail
24.	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.
25.	It shall support multiple Login Controls
26.	It shall support Guest Management.
27.	It shall support bulk username and password creation
28.	It shall support centralized Profile creation & Subscriber Provisioning
29.	It shall support Web self-care for subscriber to track usage summary
30.	It shall support different customer acquisition process for Public Wi-Fi users
31.	It shall support time bound username & password generation for Wi-Fi users
32.	It shall be able to bind the MAC of Wi-Fi users
33.	It shall have centralized Database which enables administrator easily manage database from a single point in distributed Architecture
34.	It shall allow administrator to define whether the subscriber has to be added to the existing customer database or added as a fresh customer. Multiple subscribers shall be added under same customer. Administrator can define the username & password by which the subscriber can login.
35.	It shall allow administrator to lists down the complete subscriber list in the system and allows updating or modifying subscriber information as required.
36.	Administrator can select the customer name from the list and update details.
37.	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.
38.	This shall work as interface between KSCL and City Wi-Fi user. Any prospective user coming into KSCL public hotspot shall be presented a

#	**Minimum specification**
	webpage portal giving details of Wi-Fi services, tariffs and procedure to subscribe to the services.
39.	Citizen should be able to make payment through this portal
40.	The subscriber shall be able to check his Wi-Fi account details
41.	Shall be able to change his password
42.	Shall be able to create new Wi-Fi accounts through Captive/Web portal
43.	Shall be able to display the complete information includes IP address using which the subscriber logged in as well as the MAC address of the subscriber (if MAC binding option is selected).
44.	For security reasons it shall suggest subscribers to regularly change or update their password.
45.	It shall allow subscribers to update personal details and contact information

5.1.5.10.2.1.2 Technical Specifications - WLAN Controller

#	**Minimum specification**
1	Must be compliant with IEEE CAPWAPor equivalent for controller-based WLANs.
2	Should have atleast 4 x 10 Gigabit Ethernet interface.
3	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.
4	Controller should have hot-swappable redundant power supplies.
5	Controller should be capable of supporting both 1G and 10 G SPFs on same Network I/O ports
6	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 factor, multiple controllers must be proposed to meet the requirement from day one. Proposed controller should support 1+1/N+1 redundancy from day one
7	Should be rack-mountable. Required accessories for rack mounting to be provided.
8	WLC should support AVC functionality on local switching architecture
9	WLC should support AC and DC powering options
10	WLC should support AP License Migration from one WLC to another

11	**S**hould support minimum 4000 VLANs
12	WLC should support L2 and L3 roaming for IPv4 and IPv6 clients
13	WLC should support guest-access functionality for IPv6 clients.
14	Should support IEEE 802.1p priority tag.
15	Should provide real-time radio power adjustments based on changing environmental conditions and signal coverage adjustments.
16	Should support automatic radio channel adjustments for intelligent channel switching and real-time interference detection.
17	Should support client load balancing to balance the number of clients across multiple APs to optimize AP and client throughput.
18	Should support flexible DFS to prevent additional 20/40 Mhz channels from going unused
19	Should support minimum 500 WLANs
20	Should support dynamic VLAN assignment
21	Should able to do dynamic channel bonding based on interference detected on particular channel.
22	Must support RF Management with 40 MHz and 80 Mhz channels with 802.11n & 802.11ac
23	Should provide visibility to Network airtime in order to set the airtime policy enforcement
24	Must be able to restrict the number of logins per user.
25	Should support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.
26	Should support MAC authentication to provide simple authentication based on a user's MAC address.
27	WLC Should support Rogue AP detection, classification and standard WIPS signatures.
28	The controller shall be able to detect employee device connection to Rogue Access Point and contain it automatically
29	WLC should be able to exclude clients based on excessive/multiple authentication failure.
30	Shall support AES or TKIP encryption to secure the data integrity of wireless traffic
31	Shall able to provide real time chart showing interference per access point on per radio and per-channel basis.

32	Should support AP location-based user access to control the locations where a wireless user can access the network
33	Should support Public Key Infrastructure (PKI) to control access
34	Must be able to set a maximum per-user bandwidth limit on a per-SSID basis.
35	Should support SNMPv3, SSHv2 and SSL for secure management.
36	Should support encrypted mechanism to securely upload/download software image to and from Wireless controller.
37	Should support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group
38	Should support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation
39	Should have a suitable serial console port.
40	Should have Voice and Video Call Admission and Stream prioritization for preferential QOS
41	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
42	Controller should have profiling of devices based on protocols like HTTP, DHCP and more to identify the end devices on the network.
43	Should support visibility and control based on the type of applications
44	The controller failover shall not trigger client de-authentication

5.1.5.10.2.1.3 Technical Specifications - Wireless Access Point

#	**Minimum specification**
1	Access Points proposed must be 802.11ac, Wave 2 compliant, include radios for both 2.4 GHz and 5 GHz.
2	AP should support dual band antenna ports.
3	Must have -100 dB or better Receiver Sensitivity.
4	Must support 2X2 multiple-input multiple-output (MIMO) with two spatial streams
5	Must support 802.11ac, Wave 2 and backward compatible with 802.11n standards
6	Must support datarates upto 860 Mbps on 5Ghz radio.
7	Must support 80 MHz wide channels in 5 GHz.

8	Must support WAP enforced load-balance between 2.4Ghz and 5Ghz band.
9	The Wireless Backhaul/Mesh shall operate in 5Ghz
10	Support Encrypted and authenticated connectivity between all backhaul components
11	Access point should have wired uplink interfaces including one 10/100/1000BASE-T Ethernet autosensing (RJ-45).
12	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.
13	Wireless AP Should able to detect and classify non-Wi-Fi wireless transmissions.
14	Must incorporate radio resource management for power, channel, coverage hole detection and performance optimization
15	Access point shall support powering from AC /DC/ POE/PoE+
16	Access point shall support pole, wall and Cable strand mounting options.
17	The Access point shall be IP65 or better.
18	The Access point shall support operating temperature of -40 to 65°C
19	WiFi Alliance Certification for WMM and WMM power save
20	Must support QoS and Video Call Admission Control capabilities.
21	Must support Spectrum analysis including @ 80 MHz
22	Same model AP that serves clients must be able to be dedicated to monitoring the RF environment.
23	Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
24	Must support 16 WLANs per AP for BSSID deployment flexibility.
25	Must support telnet and SSH login to APs directly for troubleshooting flexibility.

5.2 Scope of Integration:

MSI has to integrate all the existing and upcoming solutions available in city with respect to uses cases and the effective decision management perspective as mentioned below but not limited to:

5.2.1 Existing Solutions:

- Smart Lighting
- ICT Enabled Solid Waste Management
- Intelligent Transportation System
- E-Challan System

- Smart Education
- Smart Health Management System

5.2.2 Future Solutions:

- SCADA for Water
- SCADA for Energy
- Intelligent Transportation System
- E-Challan System
- Public Bike Sharing
- Smart Water Supply System

6 Project Governance and Change Management

6.1 Project Management and Governance

6.1.1 Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from MSI. It will also include key persons from other relevant stakeholders including members of KSCL and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by MSI including maintaining weekly statuses, minutes of the meetings, weekly/monthly/project plans, etc.

PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

i. Project Progress

ii. Delays, if any – Reasons thereof and ways to make-up lost time

iii. Issues and concerns

iv. Performance and SLA compliance reports;

v. Unresolved and escalated issues;

vi. Project risks and their proposed mitigation plan

vii. Discussion on submitted deliverable

viii. Timelines and anticipated delay in deliverable if any

ix. Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would also include:

i. Module development status

ii. ii. Testing results

iii. IT infrastructure procurement and deployment status

iv. Status of setting up/procuring of the Helpdesk, DC hosting

v. Any other issues that either party wishes to add to the agenda.

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

6.1.2 Helpdesk and Facilities Management Services

MSI shall be required to establish the helpdesk and provide facilities management services to support the KSCL and stakeholder department officials in performing their day- to-day functions related to this system.

MSI shall setup a central helpdesk dedicated (i.e. on premise) for the Project. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which MSI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

MSI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to KSCL's Project In-charge for Smart City Project and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however MSI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

#	Resources
1.	Operators
2.	Program Manager
3.	Solution Architect
4.	IoT Expert
5.	Command Control & Communication Centre Expert
6.	Database Expert
7.	Security Expert
8.	System Admin
9.	Network Expert
10.	GIS Expert

Note: Numbers provided for staff providing 24*7 support is excluding relievers.

6.1.3 Steering Committee

- The Steering Committee will consist of senior stakeholders from KSCL, its nominated agencies and MSI. MSI will nominate its Smart City vertical head to be a part of the Project Steering Committee
- MSI shall participate in monthly Steering Committee meetings and update Steering Committee on Project progress, Risk parameters (if any), Resource deployment and plan, immediate tasks, and any obstacles in project. The Steering committee meeting will be a forum for seeking and getting approval for project decisions on major changes etc.

- All relevant records of proceedings of Steering Committee should be maintained, updated, tracked and shared with the Steering Committee and Project Management Office by MSI.
- During the development and implementation phase of the project, it is expected that there will be at least fortnightly Steering Committee meetings. During the O&M phase, the meetings will be held at least once a quarter.
- Other than the planned meetings, in exceptional cases, KSCL may call for a Steering Committee meeting with prior notice to MSI.

6.1.4 Project Monitoring and Reporting

- MSI shall circulate written progress reports at agreed intervals to KSCL and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.
- Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. KSCL reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

6.1.5 Risk and Issue management

- MSI shall develop a Risk Management Plan and shall identify, analyse and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.
- MSI shall carry out a Risk Assessment and document the Risk profile of KSCL based on the risk appetite and shall prepare and share the KSCL Enterprise Risk Register. MSI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with KSCL.
- MSI shall monitor, report, and update the project risk profile. The risks should be discussed with KSCL and a mitigation plan be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

6.1.6 Governance procedures

MSI shall document the agreed structures in a procedures manual.

6.1.7 Planning and Scheduling

MSI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. MSI has to get the plan approved from KSCL at the start of the project and it should be updated every week to ensure tracking of the progress of the project.

The project plan should include the following:

1. The project break up into logical phases and sub-phases;
2. Activities making up the sub-phases and phases;
3. Components in each phase with milestones;
4. The milestone dates are decided by KSCL in this RFP. MSI cannot change any of the milestone completion dates. MSI can only propose the internal task

deadlines while keeping the overall end dates the same. MSI may suggest improvement in project dates without changing the end dates of each activity.

5. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
6. Start date and end date for each activity;
7. The dependencies among activities;
8. Resources to be assigned to each activity;
9. Dependency on KSCL

6.1.8 License Metering / Management

MSI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the ICCC, and DC. This may be carried out through the use of standard license metering tools.

6.2 Manpower Deployment

MSI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to KSCL and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however MSI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

#	Type of Resource	Minimum Quantity	Minimum Deployment during Implementation phase	Minimum Deployment during O & M phase
1.	Team Leader-cum-Program Manager	1	100%	100%
2.	Solution Architect	1	80%	Onsite Support to Project team on need basis
3.	IoT Expert	1	60%	Onsite Support to Project team on need basis
4.	Command and Control Expert	1	80%	Onsite Support to Project team on need basis
5.	ITMS Expert	1	50%	Onsite Support to Project team on need basis
6.	Database Expert	1	80%	100%
7.	Security Expert	1	60%	Onsite Support to Project team on need basis
8.	Systems Administrator	1	50%	100%

9.	Network Administrator	1	50%	100%
10.	GIS Expert	1	80%	100%
11.	Software Lead	1	80%	100%
12.	Quality Assurance/Testing	As required	As required	As required
13.	Programmer	As required	As required	As required
14.	Mobile App Developer	As required	As required	As required

Apart from the above mentioned manpower, MSI is required to provide suitable manpower to monitor the data feeds at command Centre and support KSCL in operationalization of the project. Total number of operators required for the project is 30 in three shifts. KSCL reserves the right to increase or decrease the number of operators. The exact role of these personnel and their responsibilities would be defined and monitored by KSCL and respective departmental personnel. MSI shall be required to provide such manpower meeting following requirements:

1. All such manpower shall be minimum graduate pass
2. All such manpower shall be without any criminal background / record.
3. KSCL 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.
4. MSI shall have to replace any person, if not found suitable for the job.
5. All the manpower shall have to undergo training from MSI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from KSCL officers on right approaches for monitoring the feeds & providing feedback to KSCL, Traffic Police and other associated government agencies.
6. Each person shall have to undergo compulsory 1 day training every month
7. 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, standard operating procedure, governance and oversight plan shall be prepared by MSI during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

The supervisors required for operationalization of the project will be provided by KSCL, as per requirements.

6.3 Change Management & Control

6.3.1 Change Orders / Alterations / Variations

a. MSI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The vendor would need to etch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of MSI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

b. Further upward revisions and or additions required to make MSI's selected equipment and installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.

c. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which MSI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by MSI without any time and cost effect to Purchaser.

6.3.2 Change Order

a. The Change Order will be initiated only in case (i) the Purchaser directs in writing MSI to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) MSI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser, (iii) the Purchaser directs in writing MSI to incorporate changes or additions to the technical specifications already covered in the Contract.

b. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.

c. Any change order comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.

d. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.

e. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by MSI for approval, MSI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the Purchaser.

6.4 Exit Management

a. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.

b. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.

c. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

6.4.1 Cooperation and Provision of Information

During the exit management period:

a. MSI will allow the KSCL or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the KSCL to assess the existing services being delivered;

b. Promptly on reasonable request by the KSCL, MSI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by MSI or sub-contractors appointed by MSI). The KSCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. MSI shall permit the KSCL or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by MSI and to assist appropriate knowledge transfer.

6.4.2 Confidential Information, Security and Data

a. MSI will promptly on the commencement of the exit management period supply to the KSCL or its nominated agency the following:

- information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
- documentation relating to Intellectual Property Rights;
- documentation relating to sub-contractors;
- all current and updated data as is reasonably required for purposes of KSCL or its nominated agencies transitioning the services to its Replacement MSI in a readily available format nominated by the KSCL, its nominated agency;
- all other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable KSCL or its nominated agencies, or its Replacement MSI to carry out due diligence in order to transition the provision of the Services to KSCL or its nominated agencies, or its Replacement MSI (as the case may be).

b. Before the expiry of the exit management period, MSI shall deliver to the KSCL or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that MSI shall be permitted to retain one copy of such materials for archival purposes only.

6.4.3 Transfer of Certain Agreements

On request by the KSCL or its nominated agency MSI shall effect such assignments, transfers, licenses and sub-licenses KSCL, or its Replacement MSI in relation to any equipment lease, maintenance or service provision agreement between MSI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the KSCL or its nominated agency or its Replacement MSI.

6.4.4 General Obligations of MSI

a. MSI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the KSCL or its nominated agency or its Replacement MSI and which MSI has in its possession or control at any time during the exit management period.

b. For the purposes of this Schedule, anything in the possession or control of any MSI, associated entity, or sub-contractor is deemed to be in the possession or control of MSI.

c. MSI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

6.4.5 Exit Management Plan

a. MSI shall provide the KSCL or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the MSA as a whole and in relation to the Project Implementation, and the Operation and Management SLA.

- A detailed program of the transfer process that could be used in conjunction with a Replacement MSI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
- plans for the communication with such of MSI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the KSCL's operations as a result of undertaking the transfer;
- (if applicable) proposed arrangements for the segregation of MSI's networks from the networks employed by KSCL and identification of specific security tasks necessary at termination;
- Plans for provision of contingent support to KSCL, and Replacement MSI for a reasonable period after transfer.

b. MSI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.

c. Each Exit Management Plan shall be presented by MSI to and approved by the KSCL or its nominated agencies.

d. The terms of payment as stated in the Terms of Payment Schedule include the costs of MSI complying with its obligations under this Schedule.

e. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.

f. During the exit management period, MSI shall use its best efforts to deliver the services.

g. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

h. This Exit Management plan shall be furnished in writing to the KSCL or its nominated agencies within 90 days from the Effective Date of this Agreement.

7 Project Implementation Schedule, Deliverables and Payment Terms

7.1 Project Implementation Schedule and Deliverables Payment Schedule

T = 14 Days from Issue of LOI or LOA

#	Milestones	Deliverables	Timelines (in months)
1	**Project Implementation Phase**		**T + 10 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 months
1.2	Requirement Study • Command Control and Communication Centre (ICCC) including Data Centre • City IT Network Infrastructure • Smart Parking Management System (SPMS)	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 (HLD & LLD) of the proposed system, HLD & LDD should be prepared by OEM	T + 2 months

#	Milestones	Deliverables	Timelines (in months)
	• Intelligent Traffic Management System (ITMS) • Environmental Monitoring System • City Web Portal & Mobile App • Enterprise GIS • City Wi-Fi • Integration of ICCC platform with existing & under-development external Systems/ Applications as per scope	Integration report for external applications	
1.3	**Phase I: Go-Live** **a.** Design, supply, installation, commissioning including interior civil work, hardware, system software, network equipment, bandwidth procurement	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from KSCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details requirement	T + 3 months
1.3	**Phase II: Go-Live** • Operationalization of Command Control & Communication Centre along with DC and DR • City IT Network Infrastructure – pan city availability of secure network for all proposed edge devices & sensors. Guidelines issued by MoUD for cyber security requirement should be adhered to for designing network for sensor & Wi-Fi traffic • GIS – Supply, installation, data migration, training & operationalization of enterprise GIS system for the city • City web-portal – Design, development, content writing, training & deployment of city web portal	1) Site Completion/readiness Report 2) Delivery Acceptance Reports from KSCL/authorized entity 3) Installation & Commissioning Reports 4) UAT/FAT and Go Live Certificate from KSCL/authorized entity 5) Training Content & Completion Certificate 6) Security Audit Certificate from Cert-In/STQC for Data Centre and Applications	T+7 Months

#	Milestones	Deliverables	Timelines (in months)
	• ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at 30% of total identified locations • Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations • Environmental Sensors - Supply, installation, commissioning, training & operationalization of Environmental sensors at sensors • Variable Messaging Board - Supply, installation, commissioning, training & operationalization of Variable Messaging Boards at 50% of total identified locations		
1.4	**Phase III: Go-Live** • ITMS – Supply, installation, commissioning, training and operationalization of ITSM components (ANPR, RLVD, SVDS, ATCS, PA, ECB) at remaining 70% of total identified locations • Wi-Fi - Supply, installation, commissioning, training & operationalization of City Wi-Fi at 50% of total identified locations • Smart Parking Solution – Supply, installation, commissioning, training & operationalization of smart parking solution at identified location • Variable Messaging Board - Supply, installation, commissioning, training	1. Site Completion/readiness Report 2. Delivery Acceptance Reports from KSCL/authorized entity 3. Installation & Commissioning Reports 4. Software Licenses details 5. UAT/FAT and Go Live Certificate from KSCL/authorized entity 6. Availability of Mobile App on Play Store & Apple App Store 7. Training Content & Completion Certificate	T + 9 months

#	Milestones	Deliverables	Timelines (in months)
	& operationalization of Variable Messaging Boards at remaining 50% of total identified locations • Mobile App – Design, development, delivery, training & installation of mobile app in android & iOS for identified services & integration with existing services of KSCL		
1.5	**Phase IV: Integration & Project Final Go-Live** Integration with external applications (existing & proposed)- ▪ Smart Lighting ▪ ICT Enabled Solid Waste Management ▪ Intelligent Transportation System ▪ E-Challan System ▪ Smart Water Supply System ▪ Smart Education ▪ Smart Health Management System ▪ E-Gov	1. UAT/FAT and Go Live Certificate from KSCL/authorized entity 2. Training Content & Completion Certificate 3. Security Audit Certificate from Cert-In/STQC 4. Source code of portal, Mobile App & customized applications	**T + 10 months = T1**
2	**Project Operation & Maintenance Phase**		**T1 + 60 months**
2.1	Operation & Maintenance	• Monthly & Quarterly SLA Reports • Adhoc Reports	T1 + 60 Months

Based on findings of the site survey activity done by MSI, MSI may propose a change in the number of sites or individual units to be deployed in each phase as well as overall scope and a consequent change in phasing. KSCL also retains the right to suo-moto change the number of sites or individual units to be deployed for each scope item. The final decision on change in phasing and related change in payment schedules shall be at the discretion of KSCL.

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 KSCL 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 KSCL'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.

7.2 Payment Schedule

The total payment shall be paid in two part (i) Capex (70% of total bid value) (ii) Opex (30% of total bid value). The further breakup of Capex and Opex shall be as under:

#	Milestones	Timelines	Payment
	Capex (70%)		
1.	Requirement study	T + 2 Months	10% of capex value
2.	Phase II : Go Live	T + 3 Months	25% of capex value
3.	Phase III : Go Live	T + 9 Months	35% of capex value
4.	Phase IV : Integration & Project Final Go-Live	T1 = T + 10 months	30% of capex value
	Opex (30%)		
5.	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 –

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

Note 2:

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

8 Annexure:

8.1 Annexure I: Bill of Material

Mentioned below is the indicative Bill of Material for each proposed project component, however the below quoted numbers are indicative only and MSI is required to access the exact requirement, location wise, for all the proposed solution components and shall accordingly size the hardware and software infrastructure requirement to meet the project objectives and SLA.

8.1.1 Pan City Network Backbone

#	Line Item	Unit of Measurement	Indicative quantity
1.	24 Core Optical Cable based last mile connectivity	As required to cover pan city	As required to cover pan city
2.	Aggregate bandwidth at DC	As required to cover pan city	As required to cover pan city

3.	Leased Circuit Bandwidth	As required to cover pan city	As required to cover pan city

8.1.2 Command Control and Communication Centre

#	Line Item	Unit of Measurement	Indicative quantity
1.	Video wall (70” in 5x2 configuration)	Unit	1
2.	Video Wall Controller	No.	1
3.	Video Wall Management Software	No.	1
4.	Cabling & Other Fixtures	Lot	1
5.	Keyboard Joystick to control PTZ Cameras	No.	10
6.	Network Access Switch	No.	1
7.	LED TV 55"	No.	3
8.	Public Address System	Set	1
9.	Audio Mixer and speaker system	Set	1
10.	Workstation Desktop with two monitors	No.	20
11.	Online UPS (sizing as per proposed solution)	No.	As per requirement (in n + n fashion)
12.	Multifunction Device	No.	2
13.	IP Phones	Set	10
14.	Public Address System	Set	1
15.	Video Conferencing software and solution	Set	1
16.	Network Colour Laser printer	No.	1
17.	Network B/W Laser Printer	No.	2
18.	Network B/W Laser Printer (Heavy Duty)	No.	1
19.	Biometric access control system	No.	As per bidder’s solution
20.	Dome cameras for internal surveillance	No.	8
21.	Fire Alarm System	Set	1
22.	Rodent Repellent system	Set	1
23.	Split Air Conditioner 2 Ton (5 star energy efficiency rating)	No.	As per requirement
24.	Site Preparation as per the RFP	Lump sum	1
25.	Workstation Furniture and Fixtures for ICCC	No.	15
26.	Revolving Chairs for office staff	No.	15
27.	Office Desk Furniture and Fixtures	No.	15
28.	Ergonomic Chairs for ICCC	No.	25
29.	Conference Table (for 10 personnel) & Chairs Set	Set	1
30.	Manpower – Operators	No.	20 in three shifts (shift distribution shall be decided by KSCL)

8.1.3 Helpdesk

#	Line Item	Unit of Measurement	Indicative quantity
1.	Hand Set	No.	5
2.	Head Set	No.	5
3.	Voice Logger	No.	1
4.	Soft telephone	No.	5
5.	Desktops	No.	5
6.	Officer Furniture and Revolving Chair	Lot	5

8.1.4 Data Centre

#	Line Item	Unit of Measurement	Indicative quantity
	Core Infrastructure		
1.	Core Router	No.	2
2.	Core Switch	No.	2
3.	Internet/ Core Router	No.	2
4.	Firewall(NGFW)	No.	2
5.	Web Security	No.	2
6.	Data Centre/EdgeSwitch	No.	As per requirement
7.	42U Network Rack	No.	As per requirement
8.	KVM Switch	No.	2
9.	Blade Chassis	No.	As per requirement
10.	Video Management Server	No.	4
11.	Video Analytics Server	No.	2
12.	Network Video Recorder	Lot	As per requirement
13.	ATCS Server	No.	2
14.	ANPR Server	No.	4
15.	RLVD Server	No.	4
16.	TARS server	No.	2
17.	Variable Message Signboard server	No.	2
18.	Smart Parking Information Management Solution Server	No.	2
19.	Environment Management server	No.	1
20.	City Wi-Fi Server	No.	2
21.	Wireless Intrusion Prevention System	No.	2
22.	Wi-Fi Controller	No.	2
23.	Automatic Call Distributor Server	No.	1
24.	Digital Voice Logger Server	No.	1
25.	GIS server	No.	2
26.	Database Server	No.	4
27.	Web Server	No.	2
28.	Server Load Balancer	No.	2
29.	SAN Switch	No.	2

#	**Line Item**	**Unit of Measurement**	**Indicative quantity**
30.	Storage (Primary)	TB	2500
31.	Tape Library	Lot	As per requirement
32.	Online UPS (sizing as per proposed solution)	No.	As per requirement (in n + n fashion)
33.	Precision Air Conditioning System for the Server Farm Area	No.	As per requirement (in n+1 fashion)
34.	Split Air Conditioner for the Auxiliary Area	No.	As per requirement
35.	Site Preparation Cost	Lump Sum	1
	Software Solutions		
36.	Server OS License	No.	As per requirement
37.	Virtualization Software License	Lot	1
38.	Database	Lot	1
39.	Web server	Lot	1
40.	Anti-virus & Anti-Spam software	Lot	1
41.	Backup software	Lot	1
42.	EMS	Lot	1
43.	Mail & Messaging Solution	Lot	1
44.	ICCC core application	Lot	1
45.	SMS Gateway with annual 200,000 SMSs	Lot	1
46.	ITMS - ACTS Software	Lot	1
47.	ITMS - Video Management Software	Lot	1
48.	ITMS - Video Analytics Software	Lot	1
49.	ITMS - ANPR Software	Lot	1
50.	ITMS - RLVD Software	Lot	1
51.	ITMS - SVD software	Lot	1
52.	ITMS – TARS	Lot	1
53.	ITMS - PA Software	Lot	1
54.	ITMS - ECB management software	Lot	1
55.	ITMS - Variable Message Software	Lot	1
56.	Environment Management	Lot	1
57.	Smart Parking Management Information System	Lot	1
58.	Centralized Wi-Fi Management Solution	No.	1
59.	City Portal	Lot	1
60.	Mobile Application	Lot	1
61.	Enterprise GIS	Unit	1
62.	Automated Call Distribution Software	Lot	1

#	Line Item	Unit of Measurement	Indicative quantity
63.	Computer Telephony Integration Software	Lot	1
64.	IVR Software	Lot	1
	Bandwidth		
65.	Aggregate bandwidth at DC	Bandwidth	As per requirement
66.	MPLS line between DC & Cloud DR	Bandwidth	As per requirement
67.	Leased circuit/bandwidth termination at field locations	Quantity	As per requirement
	Power Backup		
68.	Diesel Genset	Unit	1
	Manpower		
69.	System Administrator	No.	1
70.	Network Administrator	No.	1
71.	Database Administrator	No.	1

8.1.5 Data Recovery Centre

#	Line Item	Unit of Measurement	Indicative quantity
1.	Servers	No.	As per requirement
2.	Storage	No.	As per requirement
3.	Bandwidth	Mbps	As per requirement
4.	DC-DR license	Lot	As per requirement

8.1.6 City Wi-Fi – Field Equipment

#	Line Item	Unit of Measurement	Indicative quantity
1.	Access Point	No.	86
2.	Network Switch Ruggedized	No.	As per requirement
3.	Junction Box	No.	As per requirement
4.	Online UPS – 1 KVA (in case bidder proposes solar power, required items should be mentioned in the technical proposal)	No.	1
5.	Site Preparation Cost	Lump-sum	1

8.1.7 ITMS – Field Equipment

Total no. of locations across the city identified for implementing ITMS including ATCS, RLVD, ANPR, SVD, Surveillance, PA and ECB solution is around 50. An indicative Bill of Material required for undertaking initial stage of implementation is specified below.

#	Line Item	Unit of Measurement	Indicative quantity
1.	**ATCS**		
a.	ATCS Traffic signal controller	No.	50

#	Line Item	Unit of Measurement	Indicative quantity
b.	Vehicle Detection Camera	No.	510
c.	Countdown timer	No.	122
d.	Traffic Light Aspects – Red	No.	As per requirement
e.	Traffic Light Aspects – Green	No.	As per requirement
f.	Traffic Light Aspects – Amber	No.	As per requirement
g.	Pedestrian lamp heads – Stop	No.	As per requirement
h.	Pedestrian lamp heads – Walk	No.	As per requirement
i.	Gantry Pole including site preparation cost	No.	As per requirement
j.	Mounting Structure with poles, junction boxes	Set	As per requirement
k.	Network Switch Ruggedised	No.	As per requirement
2.	**RLVD**		
a.	Red Light Violation Detection (RLVD) sensors	Per leg	52
b.	Camera with ANPR capability	No.	89
c.	Local processing unit	No.	25
d.	Mounting structure with pole, junction boxes etc.	Set	As per requirement
e.	Network Switch Ruggedised	No.	As per requirement
3.	**SVD**		
a.	Speed Detection System for covering 2 lanes in one direction with complete subcomponents including ANPR camera, sensors, wide angle evidence camera, IR illuminator, non-intrusive speed sensor, with cabling & mounting infrastructure as required	Locations	50
4.	**Surveillance System**		
a.	Outdoor Fixed Box Camera + IR Illuminator	No.	510
b.	Outdoor PTZ Camera + IR Illuminator	No.	149
c.	ANPR Camera	No.	89
d.	Network Video Recorder	Lot	As per requirement
5.	**Traffic Accident Reporting System (TARS)**		
a.	Camera	No.	15
b.	Video Recorder	Lot	As per requirement
6.	**Public Address System**		
a.	Public Address System – IP based PA with speakers	No.	148
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structures with pole etc.	No.	As per requirement
7.	**Variable Message Sign**		
a.	Variable Message Sign Board	No.	88
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structures with pole etc.	No.	As per requirement
8.	**Emergency Call Box**		

#	**Line Item**	**Unit of Measurement**	**Indicative quantity**
a.	ECB system	No.	50
b.	UPS (required capacity)	No.	As per requirement
c.	Mounting structure with pole etc.	No.	As per requirement
9.	Junction boxes for ITMS solution	No.	As per requirement
10.	Power cables	Meter	As per requirement

8.1.8 Smart Parking – Field Equipment

#	**Line Item**	**Unit of Measurement**	**Indicative quantity**
1.	Camera Based Sensors parking sensors	No.	54
2.	Parking Information Management Software for On-Street parking	Lot	1
3.	Parking Mobile Application	Lot	1
4.	Network Switch	No.	As per requirement
5.	Pole including site preparation cost	No.	As per requirement
6.	Junction box	No.	As per requirement
7.	Site Preparation	Lump sum	1

8.1.9 Environment Sensors – Field Equipment

#	**Line Item**	**Unit of Measurement**	**Indicative quantity**
1.	Environment sensors	No.	50

8.2 Annexure II: ICCC Design Consideration

8.2.1 Key Design Considerations

Key design considerations taken into account are as follows –

- Designed for 24x7 online availability of application.
- Scalable solution on open protocols; no propriety devices/ applications
- API based architecture for Integration with other web applications and Mobile applications. Key guiding principles considered for building the integrated solution are the following:
    - Continuous adoption of rapidly evolving Technology - Technology evolves too fast and Government projects similar to Smart City with its long procurement cycles do not align naturally to adapt to this trend. Also, any changes to existing implementations require contract changes, new RFP (Request for Proposal), etc. Hence the entire system would be built to be open (standards, open API, plug-n-play capabilities), 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.
    - Selection of best solution at best rate as and when required - 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) and still aligned to open procurement practices of the Government. For this to happen, architecture should be open and vendor neutral, use commodity hardware, and designed for horizontal scale. This allows buying of commodity compute, storage, etc. only when needed at best price.
    - Distributed Access and Multi-channel service delivery -With high penetration of mobile devices and very large percentage of internet usage using mobile devices, it is imperative that the Smart City applications provide multiple channels of service delivery to its stakeholders. An important consideration is that the access devices and their screen capabilities (including browser variations) are numerous and constantly evolve. Hence, it is imperative to design the system such that the ecosystem of Smart City-integrated mobile apps also evolves.
    - Security and privacy of data - Security and privacy of data within the integrated Project will be foundational keeping in view of the sensitivity of data and critical nature of the infrastructure envisioned to be built for Smart City operations. Security and privacy of data should be fundamental in design of the system without sacrificing utility of the system. When creating a system of this scale, it is imperative that handling of the sensitivity and criticality of data are not afterthoughts, but designed into the strategy of the system from day one.
    - Provision of a Sustainable, Scalable Solution - The motive of the technological enhancements to provide a system that would be sustainable for the next few years. The expectation is that the system should sustain at least 5 years from GO-Live. The solution would be done keeping in mind the scalability of the system. The simplified procurement processes and ease of compliance is expected to lead to huge growth in contract's base.

Every component of KSCL system needs to scale horizontally to very large volume of data.

The Application Software will have the capability to scale up to tomorrow's requirements like given below:

- Managing the entire Property Life Cycle (Data Collaboration between various govt. departmental systems)
- Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with KSCL)
- API Approach- KSCL has decided to adopt Open API as the guiding paradigm to achieve the above goals. Though KSCL system would develop a portal but that would not be the only way for interacting with the KSCL system as the stakeholders via his choice of third party applications, which will provide all user interfaces and convenience via desktop, mobile, other interfaces, will be able to interact with the KSCL system. These applications will connect with the KSCL system via secure KSCL system APIs. This architectural approach has been taken as the UI based integration through a ubiquitous web portal requires manual interaction and does not fit most consumption scenarios. The following benefits are envisaged from API based integration,
    - Consumption across technologies and platforms(mobile, tablets, desktops, etc.) based on the individual requirements
    - Automated upload and download of data
    - Ability to adapt to changing taxation and other business rules and end user usage models
    - Integration with customer software (GIS, Accounting systems).
- Business Rule Driven Approach-All configurations including policy decisions, business parameters, rules, etc. shall be captured in a central place within the system. The system shall provide facility to the decision makers to add new or edit/delete existing policies or make changes with appropriate permission control and audit trace. Managing these in a central repository ensures only once source of truth is used across many application servers and reduces issues of inconsistent application behavior. Decoupling of the business parameters/rules/master data from the rest of the solution architecture and making them configurable allows for a great deal of flexibility.
- Data Distribution Service-As a future roadmap it is envisaged that the functionalities provided by the KSCL Project should be available as services that could be offered to other stakeholders on request. Keeping this in mind the system shall be able to provide data on subscription-publication basis. The organization of the information exchange between modules is fundamental to publish-subscribe (PS) systems. The PS model connects anonymous information producers (publishers) with information consumers (subscribers). The overall distributed application (the PS system) is composed of processes. The goal of the DDS architecture is to facilitate efficient distribution of data in a distributed system. Participant using DDS can ‘read’ or ‘write’ data efficiently and naturally with a typed interface. Underneath, the DDS middleware will distribute the data so that each reading participant can access the ‘most current’ values.

8.2.1.1 Guiding Architecture Principle

The IT architecture principles defined in this section are the underlying general rules and guidelines that will drive the subsequent development, use and maintenance of architectural standards, frameworks and future state target architecture.

KSCL system will be built on the following core principles:

8.2.1.1.1 Platform Approach

It is critical that a platform based approach is taken for any large scale application development, to ensure adequate focus and resources on issues related to scalability, security and data management. Building an application platform with reusable components or frameworks across the application suite provides a mechanism to abstract all necessary common features into a single layer. Hence the ICCC system is envisaged as a faceless system with 100% API driven architecture at the core of it. KSCL portal will be one such application on top of these APIs, rather than being fused into the platform as a monolithic system.

Open APIs designed to be used form the core design mechanism to ensure openness, multi-user ecosystem, specific vendor/system independence, and most importantly providing tax payers and other ecosystem players with choice of using innovative applications on various devices (mobile, tablet, etc.) that are built on top of these APIs.

8.2.1.1.2 Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

8.2.1.1.3 Data as an enterprise asset

Information is a high value asset to be leveraged across the organization to improve performance and decision making. Accurate information would ensure effective decision making and improved performance.

Effective and careful data management is of high importance and top priority should be placed on ensuring where data resides, that its accuracy can be relied upon, and it can obtained when and where needed.

8.2.1.1.4 Performance

A best of breed solution using the leading technologies of the domain should be proposed in the solution ensuring the highest levels of performance. It will also ensure that the performance of various modules should be independent of each other to enhance the overall performance and also in case of disaster, performance of one module should not impact the performance other modules.

The solution should be designed in a manner that the following can be achieved:

- Modular design to distribute the appropriate system functions on web and app server

- Increase in-memory Operations (use static operations)
- Reduce number of I/O operations and N/w calls using selective caching
- Dedicated schemas for each function making them independent and avoiding delays due to other function accessing the same schema.
- Solution should provide measurable and acceptable performance requirements for users, for different connectivity bandwidths.
- The solution should provide optimal and high performance Portal Solution satisfying response time for slow Internet connections and different browsers.

8.2.1.1.5 Scalability

The component in the architecture will be capable of being scaled up to more user requests or handling more no. of input resources in various modules. Even inclusion of additional application functionalities can be catered to by upgrading the software editions with minimal effort.

The design of the system to consider future proofing the systems for volume handling requirements

- The application functions to be divided logically and developed as Modular solution.
- The system should be able to scale horizontally & vertically.
- Data Volume- Ability to support at least 20 % projected volume growth (year on year) in content post system implementation & content migration.
- Functionality – Ability to extend functionality of the solution without significant impact to the existing functional components and infrastructure.
- Loose coupling through layered modular design and messaging - The architecture would promote modular design and layered approach with clear division of responsibility and separation of concerns at the data storage, service and integration layer in order to achieve desired interoperability without any affinity to platforms, programming languages and network technologies. The architecture has to be scalable, maintainable and flexible for modular expansion as more citizen and business services are provided through the Project. Each of the logical layers would be loosely coupled with its adjacent layers
- Data partitioning and parallel processing - Project functionality naturally lends itself for massive parallel and distributed system. For linear scaling, it is essential that entire system is architected to work in parallel within and across machines with appropriate data and system partitioning. Choice of appropriate data sources such as RDBMS, Hadoop, NoSQL data stores, distributed file systems; etc. must be made to ensure there is absolutely no "single point of bottleneck" in the entire system including at the database and system level to scale linearly using commodity hardware.
- Horizontal scale for compute, Network and storage – Project architecture must be such that all components including compute, network and storage must scale horizontally to ensure that additional resources (compute, storage, network etc.) can be added as and when needed to achieve required scale.

8.2.1.1.6 No Vendor lock-in and Replace-ability

Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/SI pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard before it can be used to ensure system is not locked in to single vendor implementation.

8.2.1.1.7 Security

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 application system should have the following

- 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 developed and adopted across the Smart City departments and systems
- 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 envisaged to access and use the system
- Appropriate authentication mechanism adhering to industry good practice of Password Policies etc.
- 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
- Data should be visible only to the authorized entity
- 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

System must implement various measures to achieve this including mechanisms to ensure security of procurement data, spanning from strong end-to-end encryption of sensitive data, use of strong PKI national standards encryption, use of HSM (Hardware Security Module) appliances, physical security, access control, network security, stringent audit mechanism, 24x7 monitoring, and measures such as data partitioning and data encryption.

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.

8.2.1.1.8 User Interface

The architecture and application solutions to be designed should promote simplicity and ease of use to the end users while still meeting business requirements. It should provide a simpler and more cost-effective solution. Reduces development time and makes the solution easier to maintain when changes in requirements occur.

This will be accomplished by the implementation of rich User Interfaces along with its integration with the DMS, Relational Data Store, Messaging and other external applications.

- Efficient and layout design are the key considerations that enhance usability which should be factored in while designing the application. Standard and consistent usability criteria must be defined. An intuitive, user friendly, well-articulated navigation method for the applications greatly enhances the usability of the application.
- Effective information dissemination
- Enhanced functionalities including personalized delivery of content, collaboration and enriching GUI features
- The load time for all web page user interfaces must satisfy both the following response time targets on 1 mbps connection:
  - 3 sec for welcome page
  - 5 sec for static pages
  - 10 sec for dynamic pages
- Ability to perform a simple search within 10 seconds on 1 mbps connectivity and a complex search (combining four terms) within 15 seconds regardless of the storage capacity or number of files and records on the system.
- Mobile Application Platform
  - Applications and services including all appropriate channels such as SMS/USSD/IVRS and development of corresponding mobile applications to the applications and services leveraging the Mobile Service Delivery Gateway (MSDG) and Mobile App Store.

- Application platform should support the following smart phone mobile OS (Android 4.0 and above, iOS 4, 5 and above, Windows Phone OS 8.0 and above, Mobile Web App)
- Support the target packaging components like (Mobile Website, Hybrid App, Native App, Web App and Application Development, Eclipse tooling platforms)
- Support the ability to write code once and deploy on multiple mobile operating systems
- Support integration with native device API
- Support utilization of all native device features
- Support development of applications in a common programing language
- Support integration with mobile vendor SDKs for app development and testing
- Support HTML5, CSS3, JS features for smartphone devices
- Support common protocol adapters for connection to back office systems (i.e. HTTP, HTTPS, SOAP, XML for format)
- Support JSON to XML or provide XHTML message transformations
- Support multi-lingual and language internalization
- Support encrypted messaging between server and client components

8.2.1.1.9 Reliability

This is a very crucial system and data are of high sensitivity, the data transfer and data management should be reliable to keep the confidence of the stakeholders. The system should have appropriate measures to ensure processing reliability for the data received or accessed through the application.

It may be necessary to mainly ensure the following

- Prevent processing of duplicate incoming files/data
- Unauthorized alteration to the Data uploaded in the KSCL system should be prevented
- Ensure minimum data loss (expected zero data loss)

8.2.1.1.10 Manageability

It is essential that the application architecture handles different failures properly; be it a hardware failure, network outage, or software crashes. The system must be resilient to failures and have the ability to restart, and make human intervention minimal.

All layers of the system such as application, infrastructure must be managed through automation and proactive alerting rather than using 100’s of people manually managing.

The entire application must be architected in such a way that every component of the system is monitored in a non-intrusive fashion (without affecting the performance or functionality of that component) and business metrics are published in a near real-time fashion. This allows data centre operators to be alerted proactively in the event of system issues and highlight these issues on a Network Operations Centre (NoC) at a granular level. The solution should be envisaged to utilize various tools and technologies for management and monitoring services. There should be management and monitoring tools to maintain the SLAs.

8.2.1.1.11 Availability

The solution design and deployment architecture will ensure that the application can be deployed in a centralized environment offering system High Availability and failover.

The solution should meet the 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.
- Network, DC, DR should be available 99.99 % time.

8.2.1.1.12 SLA driven solution

Data from connected smart devices to be readily available (real-time), aggregated, classified and stored, so as not to delay the business processes of monitoring and decision making, and will enable appropriate timely sharing across the Smart City organization.

Readily available and consumed device data will facilitate timely access of analytics reports at every level and department of the Smart City and provide timely analysis of data as well as monitoring of KPIs through SLAs resulting in effective service delivery and improved decision making.

8.2.1.1.13 Integration Architecture

This section recommends the proposed integration architecture aligning with the overarching architectural principles.

The following are the integration specifications for the various integration scenarios -

Real-time integration

All the Smart City applications will be deployed in the Data Centre while any external application of the Smart City ecosystem will reside in outside premises.

The need for an OPC Unified Architecture (OPC- UA) is felt that will facilitate KSCL in defining an enterprise integration platform. An OPC platform will help in data exchange across applications in real-time mode (both synchronous and asynchronous), promote loose coupling with ease of maintenance and change, facilitate rapid composition of complex services, achieve scalability through modularity, and improved business visibility.

The OPC UA architecture is a service-oriented architecture (SOA) and is based on different logical levels. It is an architectural style that allows the integration of heterogeneous applications & users into flexible service delivery architecture. Discrete business functions contained in enterprise applications could be organized as layers of interoperable, standards-based shared "services" that can be combined, reused, discovered and leveraged by other applications and processes.

The following are the various integration modes and techniques that could be leveraged –

- OPC Base Services are abstract method descriptions, which are protocol independent and provide the basis for OPC UA functionality. The transport layer puts these methods into a protocol, which means it serializes/deserializes the data and transmits it over the network. Two protocols are specified for this purpose. One is a binary TCP protocol, optimized for high performance and the second is Web service-oriented
- SOAP web service based interfacing technique will be leveraged as the real-time point to point synchronous integration mode with external or third party systems. The following integration points could be considered for SOAP web service based interfacing -
    - Payment gateway of the authorized banks to enable authorized users make financial transactions for the Smart City services availed by them. This should support a unified interface to integrate with all Payment Service Providers using web services over secured protocols.
    - SMS application, acting as the SMS Gateway, will make use of APIs for SMS communication to GSM network using the GSM modem, which can be both event-driven as well as time- driven. The API will be exposed to initiate the broadcasting or alert notification.
    - Social Media Apps and NoSQL data stores to exchange photos, videos and message feeds, based on interactions with Citizens and Business as well as comments/posts to inform stakeholders
    - IVR/Customer Support solution with ERP and Transactional Data Repository to exchange citizen and business demographic, registration and payment data as well as transactional data related to citizen services and municipal operations.
- Message based interfacing technique will be leveraged for real-time asynchronous integration mode. The following integration points could be considered for message based interfacing -
    - Central LDAP with ERP to synchronize member and employee user registration data
    - Payment solution and ERP to exchange payment data for tracking of beneficiary's payment transactions against different services (citizen, workers, transporter, vendor), master data (employee, vendor/supplier, location, facilities, price table)
    - Employee attendance data with ERP (HR Module) to capture data pertaining to employee location and attendance
    - Departmental applications with ERP (Asset Management module) to exchange data for procurement and maintenance of any assets or infrastructure items for each department.
    - Municipal operations application with ERP (Material Management module) to capture materials related transaction and inventory data for public works

    - Other government applications with Smart City application to exchange data for government procurement, public health schemes, welfare schemes, citizen health, etc.
- RESTful API service based interfacing technique will be leveraged for the following integration areas-
    - Access and use of various services provided by the different departments for citizens and business community will be done through a RESTful, stateless API layer.
    - Access and use of various internal functions related to operations and administration of Smart City for departmental and KSCL employees will be done through a RESTful, stateless API layer
- Data integration in batch mode will be through ETL. The following integration points could be considered for ETL based data integration -
    - Initial data migration to cleanse, validate and load the data extracted from source systems into target tables
    - Data load from all the individual transactional systems like ERP, Grievance Redressal to central enterprise data warehouse solution for aggregation, mining, dashboard reporting and analytics.

Process Integration layer of the KSCL solution will automate complex business processes or provide unified access to information that is scattered across many systems. Process Integration will provide a clean separation between the definition of the process in the process model, the execution of the process in the process manager, and the implementation of the individual functions in the applications. This separation will allow the application functions to be reused in many different processes.

An enterprise service bus (ESB) is a software architecture model used for designing and implementing the interaction and communication between mutually interacting software applications in Service Oriented Architecture. As software architecture model for distributed computing it is a variant of the more general client server software architecture model and promotes strictly asynchronous message oriented design for communication and interaction between applications. Its primary use is in Enterprise Application Integration of heterogeneous and complex landscapes. Following are the requirement for an ESB system:

- The solution should support static/deterministic routing, content-based routing, rules-based routing, and policy-based routing, as applicable in various business cases.
- The solution should have capabilities to receive input message in heterogeneous formats from various different systems, interpret those messages, process and transform those messages to generate output and feed them to various different clients as per formats applicable.
    - The solution should have features to communicate across different services, process them and expose as single aggregate service to facilitate business functionality
    - ESB should support SOA standards such as XML, XSLT, BPEL, web services standards and messaging standards.

  - ESB should support all industry standards interfaces for interoperability between different systems

There are four integration gateways envisaged as part of the solution design. The key requirements with respect to each of these are mentioned below:

SMS Gateway: SMS services are envisaged to be made available as part of the solution design. The service provider may integrate the solution with MSDG, and use the services available through it, or deploy its own SMS Gateway services at no extra charge to KSCL, but it is a mandatory requirement that all the SMS based services (alerts and notifications) should be available as part of the solution. Following are some of the key requirements for the SMS services through the solution:

- Should contain required details/information and targeted to the applicant or designated officers of tax departments and other stakeholders and users as per prevailing TRAI norms
- Facilitate access through access codes for different types of services
- Support automated alerts that allows to set up triggers that will automatically send out reminders
- Provide provision for International SMS
- Provide provision to receive messages directly from users
- Provide provision for personalized priority messages
- Resend the SMS in case of failure of the message
- Provide messaging templates

Email Services: Email services are envisaged to be made available as part of the solution design to send alerts/intimations/automated messages to registered email ids, based on preferences set up/opted by individual users. An authenticated SMTP mail service (also known as a SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution, and delivered to intended inbox. Support antispam features.

Payment Gateway: The solution is envisaged to have integration with payment gateways, to enable authorized Users make financial transactions, as per rights and privileges provided to him/her. The service provider is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the KSCL. Some of the key features of payment gateway are mentioned below:

- Should support secure integration with Payment Service Providers
- Should support a unified interface to integrate with all Payment Service Providers
- Should support integration with Payment Service Providers using web services and over HTTP/S protocol
- Should manage messages exchange between UI and payment service providers
- Should support beneficiary’s payment transactions tracking against various services
- Should support bank accounts reconciliation

- Should provide logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers
- Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country
- Should support redundant Payment Discovery
- Should submit Periodic Reconciliation Report to government entities
- Should support transaction reports to monitor and track payments
- Should support real-time online credit card authorization for merchants
- Should support compliance with emerging trends and multiple payment options such debit card, credit card, cash cards and other payment gateways
- Should provide fraud screening features
- Should support browser based remote administration
- Should support multicurrency processing and settlement directly to merchant account
- Should support processing of one-time or recurring transactions using tokenization
- Should support real time integration with SMS and emails
- IVR Services: IVR services are envisaged as part of Call Centre facility, which will be integrated with the solution, to provide information and services to the people who would contact the Call Centre: Some of the key features of the IVR services are mentioned below:
- Should provide multi-lingual content support
- Should facilitate access through access codes for different types of services
- Should support Web Service Integration
- Should support Dual Tone Multi Frequency (DTMF) using telephone touchpad - in-band and out-of-band
- Should support redirection to human assistance, as per defined rules
- Should be able to generate Data Records – (CDRs) and have exporting capabilities to other systems

There are multiple ways of integration of the solution with other systems is envisaged. These may be through Web Services, Message Queuing, File based or API based. The integration and data sharing mechanism may be either in Batch Mode or Needs basis (synchronous or asynchronous). Some of the key requirements of the interface/integration are mentioned below:

  - Interface Definition
  - Interface Owner
  - Interface Type
  - Interface Format
  - Frequency

  - Source System
  - API/Service/Store Procedure
  - Entitlement Service
  - Consuming System
  - Interface Layout (or) Schema
- Should have provision for exceptional scenarios
- Should have syntax details such as data type, length, mandatory/option, default values, range values etc.
- Error code should be defined for every validation or business rule
- Inputs and outputs should be defined
- Should be backward compatible to earlier datasets
- Data exchange should provide transactional assurance
- Response time and performance characteristics should be defined for data exchange
- The failover scenarios should be identified
- Data exchange should be auditable

Note: Bidder is free to proposed their own design to be meet the scope and SLA requirement

8.2.2 Security

Data exchange should abide by all laws on privacy and data protection Security Architecture. Proposed solution shall adhere to the guidelines & frameworks issued by GoUP/GoI from time-to-time for security for smart city solutions.

This section recommends the proposed security architecture aligning with the overarching architectural principles. The basic tenets of Smart City security architecture are the design controls that protect confidentiality, integrity and availability of information and services for all the stakeholders.

8.2.2.1 User Security and Monitoring Authentication & Authorization

A strong authentication mechanism should be considered to protect unauthorized access to the Smart City applications. Consider use of at least two of the following forms of authentication mechanism:

- Something you know, such as a password, PIN etc.
- Something you have, such as a smart card, hardware security token etc.
- Something you are, such as a fingerprint, a retinal scan, or other biometric methods

8.2.2.1.1 Levels of Authentication

Based on the security requirements the following levels of authentication should be evaluated.

- For applications handling sensitive data it is recommended that in the least one factor authentication key in the form of a password is essential. Strong password complexity rules should be enforced to ensure confidentiality and integrity of the data

- For applications handling highly sensitive data it is recommended that two factor authentication mechanisms should be considered. The first line of defense is the password conforming to the password complexity rules'. Along with the password next user has to provide a one-time password which varies for each session. One time passwords are valid for each session and it is not vulnerable to dictionary, phishing, interception and lots of other attacks. A counter synchronized One-Time Password (OTP) solution could be used for this purpose.

8.2.2.1.2 Authorization

Authorization of system users should be enforced by access controls. It is recommended to develop access control lists. Consider the following approach for developing access control list -

- Establish groups of users based on similar functions and similar access privilege.
- Identify the owner of each group
- Establish the degree of access to be provided to each group

8.2.2.2 Data Security

8.2.2.2.1 Traditional Structured Enterprise Data

KSCL should protect Integrated Project information against unauthorized access, denial of service, and both intentional and accidental modification. Data security, audit controls and integrity must be ensured across the data life cycle management from creation, accessed, viewed, updated and when deleted (or inactivated). This provides a proactive way to build defense against possible security vulnerabilities and threats, allowing errors to be corrected and system misuse to be minimized.

The implications for adhering to an effective data security and integrity guideline related to the Project are the following –

- Data security policies and standards to be developed and adopted across Kanpur Smart City applications and stakeholders
- Data security controls to be put in place to restrict access to enterprise data based on roles and access privileges. Data audit logs should be maintained for audit trail purposes. Security controls will be able to be reviewed or audited through some qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels.
- In order to adequately provide access to secured information, security needs must be identified and developed at the data level, not the application level. Database design must consider and incorporate data integrity requirements.
- Procedures for data sharing need to be established. Data integrity during data synchronization needs to be ensured across the enterprise.
- Audit Capabilities: The system provides for a system-wide audit control mechanism that works in conjunction with the RDBMS.
- Maintaining Date/Time Stamp and User Id: Every transaction, with a date and time and User ID, is captured. The system allows generating various audit reports for verification.

- Access Log: The KSCL Project should have extensive inbuilt security and access control mechanisms. Based on this, the system keeps track of the various functions accessed by any users.

8.2.2.2.2 Audit Trail & Audit Log

Audit trails or audit logs should be maintained. Log information is critical in identifying and tracking threats and compromises to the environment.

There are a number of devices and software that should be logged which include hardware & software based firewalls, web servers, authentication servers, central/domain controllers, database servers, mail servers, file servers, routers, DHCP servers etc.

It is essential to decide what activities and events should be logged. The events which ideally should be captured include

- Create, read, update and delete of confidential information;
- User authentication and authorization activities in the system, granting, modification or revoking of user access rights;
- Network or service configuration changes;
- Application process start up, shutdown or restart, abort, failure or abnormal terminations, failure of network services;
- Detection of suspicious activities such as from Intrusion Detection and Prevention system, anti- virus, anti-spyware systems etc.

8.2.2.3 Application Security

- Project must comply with the Application Security Plan and security guidelines of Government of India as applicable
- Secure coding guidelines should be followed. Secure coding guidelines should include controls against SQL injection, command injection, input validation, cross site scripting, directory traversal, buffer overflows, resource exhaustion attacks etc. OWASP Top 10 standard should be mapped in the secure coding guidelines to cover all major vulnerabilities.
- Validation checks should be incorporated into the application to detect any corruption of information through processing errors or deliberate acts.
- Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances
- Should implement secure error handling practices in the application
- Project should have Role based access, encryption of user credentials. Application level security should be provided through leading practices and standards including the following:
  - o Prevent SQL Injection Vulnerabilities for attack on database
  - o Prevent XSS Vulnerabilities to extract user name password (Escape All Untrusted Data in HTML Contexts and Use Positive Input Validation)
  - o Secure Authentication and Session Management control functionality shall be provided through a Centralize Authentication and Session Management Controls and Protect Session IDs from XSS

- Prevent Security Misconfiguration Vulnerabilities (Automated scanners shall be used for detecting missing patches, misconfigurations, use of default accounts, unnecessary services, etc. maintain Audits for updates
- Prevent Insecure Cryptographic Storage Vulnerabilities (by encrypt off-site backups, ensure proper key storage and management to protect keys and passwords, using a strong algorithm)
- Prevent Failure to Restrict URL Access Vulnerabilities (By providing authentication and authorization for each sensitive page, use role-based authentication and authorization and make authentication and authorization policies configurable
- Prevent Insufficient Transport Layer Protection Vulnerabilities (enable SSL for all sensitive pages, set the secure flag on all sensitive cookies and secure backend connections
- Prevent Id Redirects and Forwards Vulnerabilities
- For effective prevention of SQL injection vulnerabilities, MSI should have monitoring feature of database activity on the network and should have reporting mechanism to restrict or allow the traffic based on defined policies.

8.2.2.4 Infrastructure Security

The following focused initiatives to discover and remedy security vulnerabilities of the IT systems of Kanpur Smart City should be considered to proactively prevent percolation of any threat vectors -

- Deploy anti-virus software to all workstations and servers to reduce the likelihood of security threats;
- Deploy perimeter security technologies e.g. enterprise firewalls to reduce the likelihood of any security threat;
- Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages;
- Install enterprise-level e-mail anti-security software to reduce vulnerability to phishing and other e-mail security spams. This would check both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.
- Perform periodic scanning of the network to identify system level vulnerabilities
- Establish processes for viewing logs and alerts which are critical to identify and track threats and compromises to the environment. The granularity and level of logging must be configured to meet the security management requirements.
- Deploy technology to actively monitor and manage perimeter and internal information security.
- Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems. Establish process to tune, update, and monitor IDS information.
- In case of cloud deployment, cloud services can be disrupted by DDoS attacks or misconfiguration errors which have the potential to cascade across the cloud and disrupt the network, systems and storage hosting the cloud

application.

- Deploy security automation techniques like automatic provisioning of firewall policies, privileged accounts, DNS, application identity etc.

8.2.2.4.1 Network Security for Smart Devices

The core principles of security for any smart device network rest on the three most important data security concerns of confidentiality, integrity and authentication. Hence the security for smart device networks should primarily focus on the protection of the data itself and network connections between the nodes. From a network perspective, following are to be considered for designing the smart devices network -

- Protection of fair access to communication channels (i.e. media access control)
- Concealing of physical location of the nodes
- Defence against malicious resource consumption, denial of service, node capturing and node injection
- Provision for secure routing to guard the network from the effects of bad nodes
- Protection of the mobile code

Smart devices have a triple role in most networks - data collectors, processors and traffic forwarders for other devices in the network. The typical attacks for which countermeasures are to be defined and implemented are: Radio Jamming, Nodes Reporting Wrong Data, Data Aggregation Attacks and Battery Attacks.

The following guidelines need to be considered for security enhancement of smart devices and their networks:

- Use of IP-based network for smart devices
- Use of Link Layer Security for password-based access control and encryption
- Protection of smart devices nodes behind a firewall for carrying out SSL-based application data transfer and mechanism to avoid distributed DoS attacks
- Public-key-based authentication of individual devices to the network and provisioning them for secure communications
- Conformance of the security solution to the standards of IETF, IEC and IEEE to ensure maximum security and interoperability, with support for the following commonly used protocols at a minimum - IPSec/IKE, SSH and SSL/TLS

8.2.3 Software Development Lifecycle Continuous Build

The KSCL Project should be highly modular and parallel development should be carried out for faster execution using industry’s best Software Development Lifecycle practices. All application modules within the same technology platform should follow a standardized build and deployment process.

A dedicated ‘development / customization’ environment should be proposed and setup. MSI must provision separate development and testing environment for application development and testing. Any change, modifications in any module must follow industry standard processes like change management, version control and release management in large and complex application development environment.

Application source code could be maintained in source control and could be broken up into a number of projects. Source control projects are created to abstract related set of modules or feature that can be independently included in another application.

It is a mandatory to create, update and maintain all relevant documentation throughout the contract duration. Also it should be ensured that a bug tracking toll is maintained for proper tracking of all bugs fixes as per various tests conducted on the application.

8.2.4 Quality Assurance

A thorough quality check is proposed for the KSCL Project and its modules, as per standard Software Development Life Cycle (SDLC). MSI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by KSCL. MSI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a pre-defined, mutually agreed timeline. MSI must undertake the following:

- Outline the methodology that will be used for testing the system.
- Define the various levels or types of testing that will be performed for system.
- Provide necessary checklist/documentation that will be required for testing the system.
- Describe any technique that will be used for testing the system.
- Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
- Indicate / demonstrate to KSCL that all applications installed in the system have been tested.

8.2.5 Performance and Load Testing

MSI is expected to implement performance and load testing with following features:

- Testing workload profiles and test scenarios based on the various functional requirements should be defined. Application as well as system resource utilization parameters that need to be monitored and captured for each run also needs to be defined.
- Should support application testing and API testing including HTTP(s), web services, mobile applications and different web 2.0 frameworks such as Ajax/Flex/HTML5.
- MSI should perform the load testing of KSCL Project for multiple workload profiles, multiple scenarios, and user loads to handle the envisaged users of the system.
- Different activities before load testing i.e. identification of work load profiles, scenarios, information capturing report formats, creation of testing scripts, infrastructure detailing and workload profile should be prepared before the start of actual load testing exercise.
- Solution parameters needs to be tuned based on the analysis of the load

testing reports. The tuning process could be iterative until the issues are closed. Multiple load runs needs to be executed for users to simulate different scenarios, such as peak load (year end, quarter end, etc.), load generation within the LAN, Load generation across WAN or mobile network simulator while introducing configurable latency/jitter/packet loss etc.

- Should eliminate manual data manipulation and enable ease of creating data-driven tests.
- Should provide capability to emulate true concurrent transactions.
- Should identify root cause of performance issues at application or code level. Include code performance analysis to quickly pinpoint component-level bottlenecks: Slowest classes and methods, most frequently called methods, most costly (aggregate time spent for each method), response time variance etc.
- Should allow selection of different network bandwidth such as analog modems, ISDN, DSL, or custom bandwidth.
- Should be able to monitor various system components e.g. Server (OS, Web, Application & Database) Monitoring, Network (between Client & Server) Delay Monitoring, Network Devices (Firewall, Switch & Router) Monitoring during the load test without having to install any data capturing agents on the monitored servers/components
- Should correlate response times and system performance metrics to provide quick insights in to root cause of performance issues.
- Reports on following parameters (but not limited to) such as transaction response time, transaction per second (Passed), user interface rendering time, transaction per second (Failed), web transaction breakdown graphs, hits per second, throughput, HTTP responses per Second, pages downloaded per second, system infrastructure performance metrics etc.
- Should provide End-to-End system performance analysis based on defined SLAs. Should monitor resource utilization including memory leakage, CPU overload and network overload. Should have the ability to split end-to-end response time for Network & Server(s) and provide drill-down capability to identify and isolate bottlenecks.

8.3 Annexure III- Common guidelines regarding compliance of systems/equipment

1. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. MSIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
2. In case of addition/update in number of license for the products, MSI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.
3. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.
4. **None of the IT / Non-IT equipment's proposed by MSI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.**
5. All IT Components should support IPv4 and IPv6.
6. Technical Bid should be accompanied by OEM's product brochure / datasheet. MSIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.
7. MSI should ensure that only one make and model is proposed for one component in Technical Bid for example all Field cameras must belong to a single OEM and must be of the same model etc.
8. MSIs should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
9. **All equipment, parts should be original and new.**
10. The user interface of the system should be a user friendly Graphical User Interface (GUI).
11. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.
12. For custom made modules, industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empaneled vendors) to ensure that the application is free from any vulnerability; and approved by the KSCL.
13. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.
14. The Successful MSI should also propose the specifications of any additional servers / other hardware, if required for the system.
15. The indicative architecture of the system is given in this volume. The Successful

MSI must provide the architecture of the solution it is proposing.

16. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Centre equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements& SLAs defined in the Tender.

17. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 60 percent or less, disk utilisation of 75 percent or less). In case any non- standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.

18. MSI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.

19. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). KSCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.

20. All servers, active networking components (for edge level switches, please refer below for additional information), security equipment, storage systems and COTS Application proposed should be from OEMs who are amongst the top 5 for world-wide market share in terms of revenue as per IDC latest published quarterly report presence in the latest Magic Quadrant of Gartner. MSI is expected to attach the report along with the Technical Bid.

21. Cameras, Network Video Recorder (NVR) and the Video Management / Video Analytics Software should be ONVIF Core Specification ‘2.X’ or ‘S’ compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.

22. MSI shall place orders on various OEMs directly and not through any sub-contractor / partner. All licenses should be in the name of the KSCL.

8.4 Annexure IV- Tentative List of Locations

A. Wi-Fi location in city:

S. No	Area within the city	Locality
1	Kanpur Development Authority (KDA)	Harsh Nagar
2	Kanpur Municipal Corporation (KMC)	Harsh Nagar
3	KMC Zonal - 1 Office	Civil Line
4	KMC Zonal - 2 Office	Krishna Nagar
5	KMC Zonal - 3 Office	Kidwai Nagar
6	KMC Zonal - 4 Office	Motizheel
7	KMC Zonal - 5 Office	Govind Nagar
8	KMC Zonal - 6 Office	Lajpat Nagar
9	RTO Office	Sarvodaya Nagar
10	Kanpur Electricity Supply Company Ltd (KESCO) Office	Khyora Nagar
11	Kanpur Head Post Office-1 Nawabganj	Vishnu Puri
12	Kanpur Head Post Office-2 Kanpur Cantt	Down Town
13	GPO Bada Chauraha	Civil Line
14	Anwar Ganj SO	Anwar Gnaj
15	Collectorate Kanpur	Sirsaiya Ghat Rd
16	Fazal Ganj Chauraha	Fazal Ganj
17	Company Bagh Chauraha	Kalasi Line
18	Gumti No.5 Chauraha	Darshan Purwa
19	Chawla Market Chauraha	Govind Nagar
20	Bada Chauraha	Mall Road
21	Kakadeo Chauraha	Kakadeo,
22	Arya Nagar Kamal Chauraha	Arya Nagar
23	Kanpur Interstate Bus Station	Cooperganj
24	Allen Park Bus Terminal	Nawabganj
25	Kanpur Central Bus Station	Harris Ganj, Mirpur
26	Kargil Park	Harsh Nagar
27	Shaheed park	Kidwai Nagar
28	Phool Bagh	Civil Line
29	Nana Rao Park	Mall Road, Civil Lines

S. No	Area within the city	Locality
30	Gautam Buddha Park	Kalyanpur
31	Virendra Smriti Business park	Civil Line
32	Musical Fountain Park	Harsh Nagar
33	Guru Nanak Complex	Ashok Nagar
34	Naveen Market	Mall Rd, Parade
35	Sisamau Market	Harsh Nagar
36	PPN Market	Colonelganj
37	Meston Road Leather Market	patkapur
38	Mall Road	Mall Road
39	Kanpur Central Railway Station- Gate 1	Mirpur
40	Kanpur Central Railway Station -Gate 2	Mirpur
41	Kanpur Nagar District Court	Civil Line
42	SBI Main Branch (HQ)	Near Reserve Bank Civil Lines
43	Allahabad Zonal Office	Civil Line
44	Kanpur Zoological Park	Nawabganj
45	J.K Temple	Sarvodaya Nagar
46	Green Park Stadium	Permat
47	Regency Hospital	Sarvodaya Nagar
48	Kanpur Medical Centre	Lajpat Nagar
49	Kulwanti Hospital and Research Centre	Kakadeo,
50	Rama Hospital and Research Centre	Khyora
51	Ratnadeep Hospital and Research Centre	Rawat pur
52	Central Library	Kalyanpur
53	Municipal Library	Permat
54	Ram Krishna Mission Library	Jawahar Nagar
55	HBTI Library	Nawabganj
56	Chandra Shekhar Azad University Of Agriculture & Technology	Nawabganj
57	Chhatrapati Shahu Ji Maharaj University	Grand Trunk Road
58	Indian Institute Of Technology	Kalyanpur
59	G S V M Medical College	Sarvodaya Nagar
60	PSIT College of Engineering (PSITcoe)	Bhauti
61	Kanpur Institute Of Management	Harsh Nagar

S. No	Area within the city	Locality
62	Government Polytechnic Kanpur	Khyora
63	Institute of Business Management	Kalyanpur
64	Institute of Chartered Accountants of India	Civil Line
65	Deendayal Upadhyaya Institute of Management and Higher Studies	Swaroop Nagar
66	Sharda Institute of Management & Technology, Kanpur	Naramau
67	Allenhouse Institute of Technology	Kulgaon Road Rooma
68	National Sugar Institute, Kalyanpur, Kanpur.	G.T. Road
69	University Institute of Engineering and Technology, Kanpur University	Rawatpur Main Rd
70	Government leather Institute	Nawabganj
71	C.S.A. University of Agriculture & Technology	Nawabganj
72	Indian Institute of Pulses Research, Kalyanpur, Kanpur	Kalyanpur
73	Institute of Research Development and Training	Vikas Nagar
74	Forest Training Institute	Kidwai Nagar
75	Near Sagar Market	General Ganj
76	Lilamani Hospital	Civil Line
77	Padam Tower	Civil Line
78	Raina Market	Khalasi Line
79	National Informatics Centre	Civil Lines
80	Bank Of India - Kanpur Main Branch	General Ganj
81	Dayanand Anglo - Vedic College	Green Park, Civil Lines
82	Dayanand Girls P.G. College	Permat
83	Gwaltoli Market	Khalasi Line
84	DAV College, Kanpur	Civil Lines
85	Macrobert Hospital	Permat
86	D M Office Kanpur	Civil Lines

B. Intelligent Traffic Management System:

S. No.	Junction Name	Locations		Junction Details	Apprx. Traffic Movement: nos of Cars/ day (Peak time)
		Latitude/	Longitude		
1	Rama devi Chauraha	26°24'41.6"N	80°23'12.3"E	4 Way Junction	3868
2	PAC Mod Chauraha	26°24'16.3"N	80°21'26.5"E	4 Way Junction	3205
3	Taat Mill Chauraha	26°26'54.6"N	80°20'37.3"E	4 Way Junction	6643

S. No.	Junction Name	Locations		Junction Details	Apprx. Traffic Movement: nos of Cars/ day (Peak time)
		Latitude/	Longitude		
4	Apheem Koti Chauraha	26°27'20.4"N	80°20'02.3"E	4 Way Junction	4617
5	Zareeb Chawki	26°27'46.8"N	80°19'22.8"E	5 Way Junction	8483
6	Gumti No.5 Chauraha	26°28'08.2"N	80°19'00.6"E	4 Way Junction	4789
7	Coca cola Chaoouraha	26°28'18.9"N	80°18'50.2"E	4 Way Junction	4812
8	Gol Chauraha	26°28'47.5"N	80°18'21.3"E	3 Way Junction	4142
9	Rawatpur Tiraha	26°28'55.6"N	80°18'04.3"E	3 Way Junction	4402
10	Sharda Nagar Tiraha	26°29'14.7"N	80°17'29.6"E	3 Way Junction	4411
11	Gurudev Palace Crossing	26°29'28.0"N	80°17'08.0"E	4 Way Junction	5264
12	Kalyanpur Crossing	26°30'11.1"N	80°15'11.3"E	3 Way Junction	2702
13	Bithoor Tiraha	26°31'34.7"N	80°15'35.5"E	3 Way Junction	2867
14	Rocket Tiraha	26°28'57.1"N	80°18'51.2"E	3 Way Junction	4479
15	Narona Chauraha	26°27'40.1"N	80°22'08.6"E	5 Way Junction	6499
16	Phool Bagh Chauraha	26°28'06.8"N	80°21'36.6"E	5 Way Junction	7474
17	Charlees Tiraha	26°28'15.6"N	80°21'29.4"E	3 Way Junction	6980
18	Meghdoot Tiraha	26°28'22.7"N	80°21'05.6"E	3 Way Junction	7178
19	Bada (Bara) Chauraha	26°28'25.6"N	80°20'49.4"E	6 Way Junction	5483
20	Karset Chauraha	26°28'27.4"N	80°20'41.0"E	4 Way Junction	5563
21	Lal Imli Chauraha	26°28'33.7"N	80°20'22.6"E	4 Way Junction	4713
22	Colonel Ganj Tiraha	26°28'39.6"N	80°20'08.8"E	3 Way Junction	4412
23	Bakar Mandi Dhal Chauraha	26°28'29.8"N	80°19'56.9"E	4 Way Junction	4026
24	Eidgah Chauraha	26°28'32.6"N	80°19'35.2"E	4 Way Junction	5359
25	Harsh Nagar Tiraha	26°28'34.2"N	80°19'29.8"E	3 Way Junction	4506
26	Benajhabar Tiraha	26°28'38.9"N	80°19'25.3"E	3 Way Junction	4350
27	Moti Jheel Chauraha	26°28'44.7"N	80°18'54.4"E	4 Way Junction	4271
28	Moti Jheel Gate Chauraha	26°28'44.8"N	80°19'04.2"E	4 Way Junction	4022
29	Post-Martam House Tiraha	26°28'45.7"N	80°18'39.3"E	3 Way Junction	3774
30	Hallet Hospital Gate Tiraha	26°28'45.7"N	80°18'39.3"E	3 Way Junction	5418
31	Sarsaiya Ghat Chouraha	26°28'45.3"N	80°18'45.1"E	4 Way Junction	2612
32	Mahila Thana Tiraha	26°28'45.0"N	80°21'02.6"E	3 Way Junction	3854
33	D.A.V College Chauraha	26°28'47.5"N	80°20'58.6"E	4 Way Junction	2380
34	Green Park Chauraha/Stock Exchange Chauraha	26°28'54.8"N	80°20'42.4"E	4 Way Junction	5563
35	Merchant Chamber Tiraha	26°28'56.4"N	80°20'37.0"E	3 Way Junction	3461
36	Tafco (parmat) Chauraha	26°29'11.4"N	80°20'19.4"E	4 Way Junction	2345
37	Bhairo Ghat (Khalasi Line) Chauraha	26°29'22.6"N	80°19'50.5"E	4 Way Junction	5064
38	Rave three Mall Chauraha	26°29'25.9"N	80°19'39.8"E	4 Way Junction	6720
39	Rani Ghat Chauraha	26°29'30.2"N	80°19'28.1"E	4 Way Junction	4120
40	Company Bagh Chauraha	26°29'27.4"N	80°18'58.0"E	5 Way Junction	5128
41	Jajmau (Beema) Chauraha	26°25'44.0"N	80°24'09.3"E	4 Way Junction	4599
42	JK Pratham Chauraha	26°25'21.2"N	80°23'47.1"E	4 Way Junction	2390
43	Harjendra Nagar Chauraha	26°24'58.2"N	80°23'32.2"E	4 Way Junction	3994
44	Shyam Nagar Chauraha	26°24'54.3"N	80°21'49.2"E	4 Way Junction	4960

S. No.	Junction Name	Locations		Junction Details	Apprx. Traffic Movement: nos of Cars/ day (Peak time)
		Latitude/	Longitude		
45	Yashoda Nagar Chauraha	26°24'37.0"N	80°19'45.0"E	4 Way Junction	5991
46	Noubasta Chauraha	26°25'16.9"N	80°19'08.7"E	4 Way Junction	5295
47	Yadav Market Barra Chouraha	26°25'39.8"N	80°18'23.0"E	4 Way Junction	5832
48	L.M.L Chouraha	26°26'42.0"N	80°15'29.3"E	4 Way Junction	3324
49	Gas Plant Tiraha			3 Way Junction	2131
50	Steel Plant Tiraha	26°27'29.5"N	80°13'10.3"E	3 Way Junction	3114
51	Ghantaghar Junction	26°27'26.2"N	80°20'59.6"E	8 Way Junction	14351
52	KoperGanj Tiraha	26°27'39.0"N	80°20'28.0"E	3 Way Junction	3139
53	Deputy Padaav Chauraha	26°27'44.6"N	80°20'11.9"E	4 Way Junction	3726
54	Fazal Ganj Chauraha	26°27'44.5"N	80°18'32.5"E	4 Way Junction	4081
55	Vijay Nagar Chauraha	26°27'41.7"N	80°17'38.9"E	4 Way Junction	5744
56	I.T.I Tiraha	26°28'29.2"N	80°18'13.8"E	3 Way Junction	3904
57	Mariyampur Chauraha	26°27'55.4"N	80°18'23.4"E	4 Way Junction	4366
58	Bank of Baroda Chauraha	26°27'51.5"N	80°18'28.5"E	4 Way Junction	3374
59	Chawla Market Chauraha	26°26'57.0"N	80°18'33.6"E	4 Way Junction	3199
60	Deep Takies Tiraha	26°26'29.4"N	80°18'32.2"E	3 Way Junction	3219
61	Saket Nagar Tiraha	26°26'02.7"N	80°18'30.8"E	3 Way Junction	3522
62	Sachan Guest House Chauraha	26°08'53.7"N	80°10'13.0"E	4 Way Junction	5126
63	Double Puliya Tiraha	26°28'16.0"N	80°17'23.6"E	3 Way Junction	5167
64	Shastri Chowk Chauraha	26°28'09.7"N	80°17'27.9"E	4 Way Junction	4419
65	Bara Devi Chauraha	26°26'22.0"N	80°19'30.7"E	4 Way Junction	7596
66	Bakar Ganj Chauraha	26°26'27.8"N	80°20'17.7"E	4 Way Junction	5218
67	Baagahi Chawk Tiraha	26°26'14.4"N	80°20'12.0"E	3 Way Junction	4247
68	Kidwai Nagar Chauraha	26°25'58.8"N	80°20'11.9"E	4 Way Junction	4803
69	Kidawai Nbagar Side No.1 Chauraha	26°25'52.8"N	80°20'11.4"E	4 Way Junction	3939
70	Moolganj Chauraha	26°27'59.2"N	80°20'50.1"E	4 Way Junction	2645
71	Sadbhawana Chawki Chauraha	26°52'23.5"N	80°59'45.0"E	4 Way Junction	4722
72	Chetna Chauraha	26°28'30.4"N	80°21'11.9"E	4 Way Junction	2454

C. CCTV Camera Locations:

S. No.	Solution Requirement	Indicative no. of locations
1	PTZ + Fixed Box Camera (including Critical Locations)	148+ 507
2	Automatic Number Plate Recognition	88
3	Red Light Violation Detection	52

D. City Exit Points:

S.No.	City Exit Point Name	Location
1	Indian Oil Petrol Pump, G.T Road	Naramau Kchhar
2	Maina Wati Marg	Bithoor
3	Jhari Baba Mod	Civil Lines
4	Pan Chakki Crossing	Civil Lines
5	Taatmil Chauraha, G.T Road	Cooperganj
6	Jagai Purwa Chowk, Lal Banglaw Road	J.K Puri,
7	2 Purani Chungi Jajmau,Tagore Town,	Jajmau North
8	Kanpur Ganga Bridge, Kanpur Road	Jajmau North
9	Bharat Petroleum, G.T Road	Rooma Village Chakeri
10	Anoop Telecom Chowk, sungawan Road	Sangawan
11	Pandu River Bridge, Hamirpur Road	Bingawan
12	Ram Gopal Chauraha Meharwan Singh ka Purwa	Balipurwa Bingawan
13	Jhasi Kanpur Highway Bridge	Bhautipratappur
14	New Shivli Road	Kalyanpur
15	Jarauli Phase 1 Arra Road	Barra
16	Rooma GT Road	Chakeri Ward
17	Chatmara Chakeri Road	Kulgaon Road
18	Sanigawan Road	Sanigawan
19	Koyla Nagar Chowki	Koyla nagar
20	Arra Road	Hanspuram, Naubasta

S.No.	City Exit Point Name	Location
21	Ram Gopal Chauraha	Jarauli
22	Panki Power house	Ganga Ganj
23	Panki Ratanpur Road	Ratanpur Colony
24	Kalyanpur to Bithoor Road	Kalyanpur
25	Jajmau Bridge	Jajmau National Highway 25
26	Jajmau water treatment Wala Road	Jajmau

E. Location of camera’s PAS , VMS and FRS system (Edge analytics with AI and continuous learning)

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
1	Rama devi Chauraha	4 Way Junction	1	4	1	1	1	1	1
2	PAC Mod Chauraha	4 Way Junction	1	4	1	1	1	1	1
3	Taat Mill Chauraha	4 Way Junction	1	4	1	1	1	1	1
4	Apheem Koti Chauraha	4 Way Junction	1	4	1	1	1	1	1
5	Zareeb Chawki	5 Way Junction	1	5	1	1	1	1	
6	Gumti No.5 Chauraha	4 Way Junction	1	4	1	1	1	1	1
7	Coca cola Chaoouraha	4 Way Junction	1	4	1	1	1	1	1
8	Gol Chauraha	3 Way Junction	1	3	1	1	1	1	1
9	Gutaiya Crossing Tiraha	3 Way Junction	1	3		1	1	1	1
10	Rawatpur Tiraha	3 Way Junction	1	3	1	1	1	1	1
11	Sharda Nagar Tiraha	3 Way Junction	1	3			1		
12	Gurudev Palace Crossing	4 Way Junction	1	4	1	1	1	1	1
13	Kalyanpur Crossing	3 Way Junction	1	3	1	1	1	1	1
14	Bithoor Tiraha	3 Way Junction	1	3	1		1	1	1
15	IIT Gate Tiraha	3 Way Junction	1	3			1	1	
16	Rocket Tiraha	3 Way Junction	1	3	1	1	1	1	1
17	Narona Chauraha	5 Way Junction	1	5	1	1	1	1	
18	Phool Bagh Chauraha	5 Way Junction	1	5	1	1	1	1	1
19	Charlees Tiraha	3 Way Junction	1	3	1	1	1	1	
20	Meghdoot Tiraha	3 Way Junction	1	3	1	1	1	1	1
21	Bada (Bara) Chauraha	6 Way Junction	1	6	1	1	1	1	1
22	Karset Chauraha	4 Way Junction	1	4	1	1	1	1	1
23	Lal Imli Chauraha	4 Way Junction	1	4		1	1		
24	Colonel Ganj Tiraha	3 Way Junction	1	3	1	1	1	1	1
25	Bakar Mandi Dhal Chauraha	4 Way Junction	1	4	1	1	1	1	1

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
26	Eidgah Chauraha	4 Way Junction	1	4			1		
27	Harsh Nagar Tiraha	3 Way Junction	1	3	1	1	1	1	1
28	Benajhabar Tiraha	3 Way Junction	1	3			1		
29	Moti Jheel Chauraha	4 Way Junction	1	4	1	1	1	1	1
30	Moti Jheel Gate Chauraha	4 Way Junction	1	4			1		
31	Post-Martam House Tiraha	3 Way Junction	1	3			1		
32	Hallet Hospital Gate Tiraha	3 Way Junction	1	3	1		1	1	1
33	Sarsaiya Ghat Chouraha	4 Way Junction	1	4	1	1	1	1	
34	Mahila Thana Tiraha	3 Way Junction	1	3			1		
35	D.A.V College Chauraha	4 Way Junction	1	4	1		1	1	1
36	Green Park Chauraha/Stock Exchange Chauraha	4 Way Junction	1	4	1	1	1	1	1
37	Merchant Chamber Tiraha	3 Way Junction	1	3		1	1		
38	Tafco (parmat) Chauraha	4 Way Junction	1	4			1		
39	Bhairo Ghat (Khalasi Line) Chauraha	4 Way Junction	1	4	1	1	1	1	1
40	Rave three Mall Chauraha	4 Way Junction	1	4	1		1	1	1
41	Rani Ghat Chauraha	4 Way Junction	1	4			1		
42	Company Bagh Chauraha	5 Way Junction	1	5	1	1	1	1	1
43	Jajmau (Beema) Chauraha	4 Way Junction	1	4	1	1	1	1	1
44	JK Pratham Chauraha	4 Way Junction	1	4			1		
45	Harjendra Nagar Chauraha	4 Way Junction	1	4	1	1	1	1	1
46	Shyam Nagar Chauraha	4 Way Junction	1	4	1	1	1	1	1
47	Yashoda Nagar Chauraha	4 Way Junction	1	4	1		1	1	1
48	Noubasta Chauraha	4 Way Junction	1	4	1	1	1	1	1
49	Yadav Market Barra Chouraha	4 Way Junction	1	4	1	1	1	1	1
50	L.M.L Chouraha	4 Way Junction	1	4	1		1	1	1
51	Gas Plant Tiraha	3 Way Junction	1	3			1		
52	Steel Plant Tiraha	3 Way Junction	1	3	1		1	1	1

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
53	Ghantaghar Junction	8 Way Junction	1	8	1	1	1	1	1
54	KoperGanj Tiraha	3 Way Junction	1	3			1		
55	Deputy Padaav Chauraha	4 Way Junction	1	4	1	1	1	1	1
56	Fazal Ganj Chauraha	4 Way Junction	1	4	1	1	1	1	
57	Vijay Nagar Chauraha	4 Way Junction	1	4	1	1	1	1	1
58	I.T.I Tiraha	3 Way Junction	1	3			1		
59	Mariyampur Chauraha	4 Way Junction	1	4	1	1	1	1	1
60	Bank of Baroda Chauraha	4 Way Junction	1	4	1		1	1	1
61	Chawla Market Chauraha	4 Way Junction	1	4		1	1		
62	Deep Takies Tiraha	3 Way Junction	1	3	1	1	1	1	1
63	Saket Nagar Tiraha	3 Way Junction	1	3			1		
64	Sachan Guest House Chauraha	4 Way Junction	1	4	1	1	1	1	1
65	Double Puliya Tiraha	3 Way Junction	1	3			1		
66	Shastri Chowk Chauraha	4 Way Junction	1	4	1	1	1	1	1
67	Bara Devi Chauraha	4 Way Junction	1	4	1	1	1	1	1
68	Bakar Ganj Chauraha	4 Way Junction	1	4	1	1	1	1	
69	Baagahi Chawk Tiraha	3 Way Junction	1	3	1		1	1	
70	Kidwai Nagar Chauraha	4 Way Junction	1	4	1	1	1	1	1
71	Kidawai Nbagar Side No.1 Chauraha	4 Way Junction	1	4			1		
72	Moolganj Chauraha	4 Way Junction	1	4	1	1	1	1	1
73	Sadbhawana Chawki Chauraha	4 Way Junction	1	4			1		
74	Chetna Chauraha	4 Way Junction	1	4			1		
75	IMA Tiraha	3 Way Junction	1	3			1		1
76	Macharli Gate Tiraha	3 Way Junction	1	3			1		
77	Swarup Nagar Chauraha	4 Way Junction	1	4			1	1	1
78	Banns Mandi Chauraha	4 Way Junction	1	4		1	1		
79	Chandrika Devi Mandir Chauraha	4 Way Junction	1	4			1		1
80	Snageet Talkies Tiraha	3 Way Junction	1	3			1	1	

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
81	P Road Tiraha	3 Way Junction	1	3		1	1		
82	Darshan Purva Chauraha	4 Way Junction	1	4			1		
83	Khoya Mandi Tiraha	3 Way Junction	1	3			1		
84	Chaar Kambha Chauraha	4 Way Junction	1	4			1		1
85	Naahariya Tiraha	3 Way Junction	1	3			1		
86	MIG Tiraha	3 Way Junction	1	3			1		
87	Bhatia Tiraha	3 Way Junction	1	3		1	1		
88	Pandu Nagar Chauraha	4 Way Junction	1	4			1		1
89	Kabadi Market Chauraha	4 Way Junction	1	4		1	1		
90	DBS Tiraha	3 Way Junction	1	3			1		
91	Nand Lal Chauraha	4 Way Junction	1	4		1	1		
92	Devki Talkies Chauraha	4 Way Junction	1	4		1	1		1
93	Neer Jheer Chauraha	4 Way Junction	1	4			1		
94	Shashtri Nagar(Galla Mandi Chauraha)	4 Way Junction	1	4		1	1		
95	Vijay Nagar Fal Mandi Tiraha	3 Way Junction	1	3			1		1
96	Fire Service (Fajalganj) Tiraha	3 Way Junction	1	3			1		
97	C.T.I Tiraha	3 Way Junction	1	3		1	1		
98	Janta Nagar Tiraha	3 Way Junction	1	3			1		1
99	Military Camp Chauraha	4 Way Junction	1	4			1	1	
100	Gau Shala Pratham Chauraha	4 Way Junction	1	4		1	1		
101	Gau Shala Second Chauraha	4 Way Junction	1	4		1	1		
102	Keshav Nagar Chauraha	4 Way Junction	1	4			1	1	1
103	Shanidev Mandir Tiraha	3 Way Junction	1	3			1		
104	Hanuman Mandir/Trimurti Mandir Mod Chauraha	4 Way Junction	1	4			1		1
105	Sainik Chauraha	4 Way Junction	1	4			1		
106	Baans Mandi Chauraha	4 Way Junction	1	4			1		
107	Rajeev Petrol Pump Chauraha	4 Way Junction	1	4		1	1		1

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
108	Gopala Tiraha	3 Way Junction	1	3			1		
109	Sales Tax Chauraha	4 Way Junction	1	4			1		
110	Arya Nagar Chauraha	4 Way Junction	1	4			1	1	1
111	Ashok Nagar Chauraha	4 Way Junction	1	4			1		
112	Brahm Nagar Chauraha	4 Way Junction	1	4			1		
113	Ram Bagh Chauraha	4 Way Junction	1	4			1	1	
114	Lenin Park Chauraha	4 Way Junction	1	4		1	1		
115	Silvarton Tiraha	3 Way Junction	1	3			1		1
116	MG College Chauraha	4 Way Junction	1	4		1	1	1	
117	Pashupati Nagar Chauraha	4 Way Junction	1	4			1		1
118	Mainawati Marg Tiraha	3 Way Junction	1	3		1	1		
119	Singhpur Mod	3 Way Junction	1	3			1	1	1
120	Swarup Nagar Chauraha	4 Way Junction	1	4		1	1		
121	Namak Factory Chauraha	4 Way Junction	1	4			1		1
122	6 Bagaliya Chauraha	4 Way Junction	1	4			1		
123	Indian Oil Petrol Pump, G.T Road	Exit Point	1	2		1	1	1	1
124	Maina Wati Marg	Exit Point	1	2		1	1	1	1
125	Jhari Baba Mod	Exit Point	1	2		1	1	1	1
126	Pan Chakki Crossing	Exit Point	1	2		1	1	1	1
127	Taatmil Chauraha, G.T Road	Exit Point	1	2		1	1	1	1
128	Jagai Purwa Chowk, Lal Banglaw Road	Exit Point	1	2		1	1	1	1
129	2 Purani Chungi Jajmau,Tagore Town,	Exit Point	1	2		1	1	1	1
130	Kanpur Ganga Bridge, Kanpur Road	Exit Point	1	2		1	1	1	1
131	Bharat Petroleum, G.T Road	Exit Point	1	2		1	1	1	1
132	Anoop Telecom Chowk, sungawan Road	Exit Point	1	2		1	1	1	1
133	Pandu River Bridge, Hamirpur Road	Exit Point	1	2		1	1	1	1
134	Ram Gopal Chauraha Meharwan Singh ka Purwa	Exit Point	1	2		1	1	1	1

S.No	Name of Junction	Junction Type	PTZ	Fixed	RLVD	ANPR	Public Addressing	VMS	FRS
135	Jhasi Kanpur Highway Bridge	Exit Point	1	2		1	1	1	1
136	New Shivli Road	Exit Point	1	2		1	1	1	1
137	Jarauli Phase 1 Arra Road	Exit Point	1	2		1	1	1	1
138	Rooma GT Road	Exit Point	1	2		1	1	1	1
139	Chatmara Chakeri Road	Exit Point	1	2		1	1	1	1
140	Sanigawan Road	Exit Point	1	2		1	1	1	1
141	Koyla Nagar Chowki	Exit Point	1	2		1	1	1	1
142	Arra Road	Exit Point	1	2		1	1	1	1
143	Ram Gopal Chauraha	Exit Point	1	2		1	1	1	1
144	Panki Power house	Exit Point	1	2		1	1	1	1
145	Panki Ratanpur Road	Exit Point	1	2		1	1	1	1
146	Kalyanpur to Bithoor Road	Exit Point	1	2		1	1	1	1
147	Jajmau Bridge	Exit Point	1	2		1	1	1	1
148	Jajmau water treatment Wala Road	Exit Point	1	2		1	1	1	1
			148	**507**	**52**	**88**	**148**	**88**	**88**

8.5 Annexure V: Standards

Annex-A (BioMetrics Standard)

Annex-B (Digital Preservation Standards)

Annex-C (Localisation and Language Technology Standard)

Annex-D (Metadata and Data Standards)

Annex-E (Mobile Governance)

Annexure-F (GIGW)

Annex-G (Open APIs)

Annex-H (Internet of Things)

Annex-I (Smart Parking)

Annex-J (Public WI-FI)

Annex-H (Disaster Management)

Annex-A (BioMetrics Standard)

BioMetrics Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes:

	o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.

It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard.

	The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.

In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of botheyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

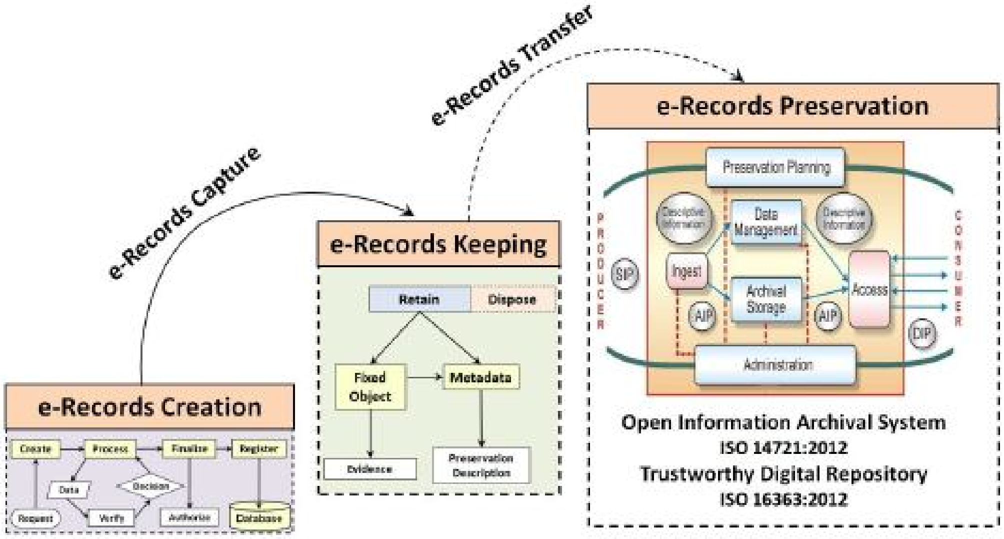
Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of OpenType fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard

	o Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features. PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

Annex-C (Localisation and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard.The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.

Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage. This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible witheach other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Suchencoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

Annex-D (Metadata and Data Standards)

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update

- Identification of attributes of the Code directories

- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers

- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification

- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-

standards-for-e-governance/)

Rerefrence Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land

    Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009
14. ANSI92 Standard

Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion users in the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. **Creation of Mobile Services Delivery Gateway (MSDG)**

   MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

   Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

   To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

   a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

   b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

   c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. Guidelines to deliver public services round-the-clock to the users using m-Governance
b. Guidelines to develop standard based mobile solutions
c. Guidelines to integrate the mobile applications with the common e-Governance infrastructure

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILE SEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

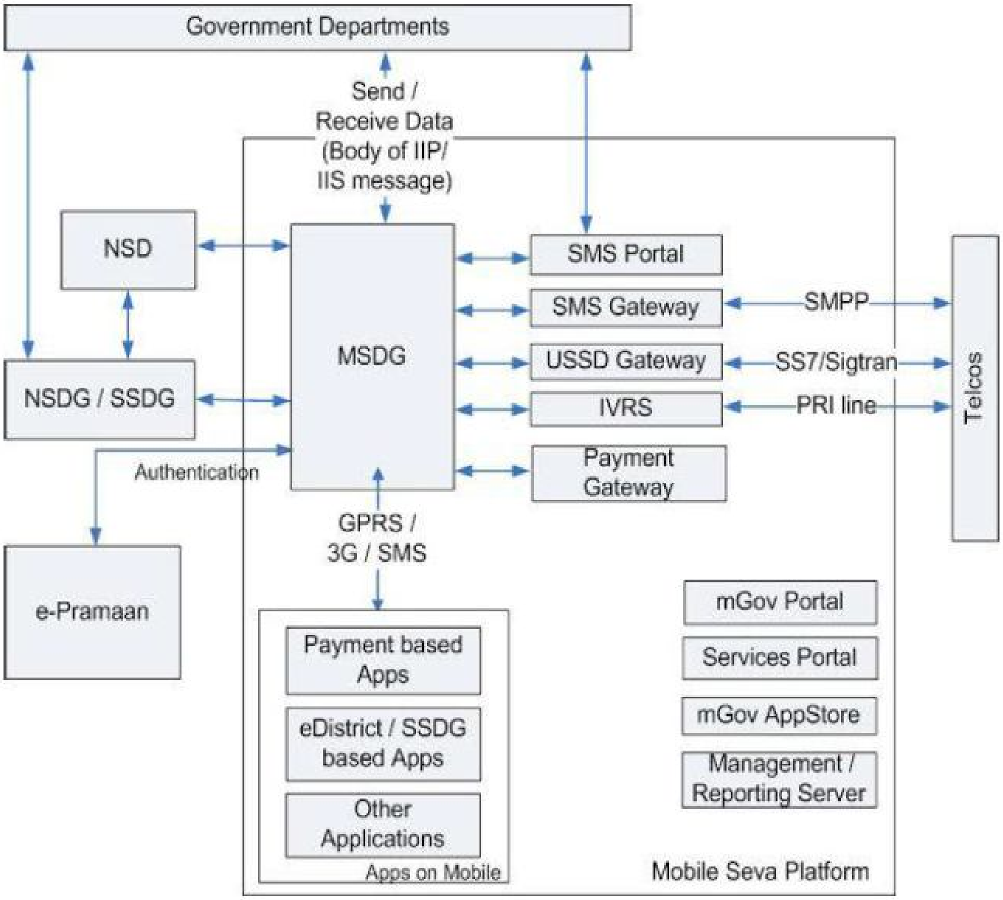


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

Mobile Application (m-Apps)

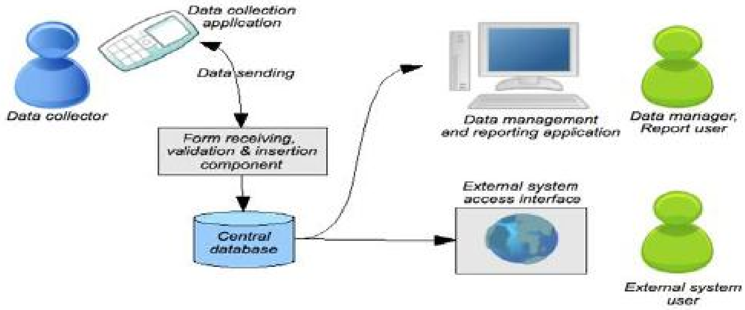
Mobile application software is applications software developed for handheld devices, such as mobile

phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**
   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**

Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:


Data collection application
Data sending
Data collector
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Markup Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to

interact with the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

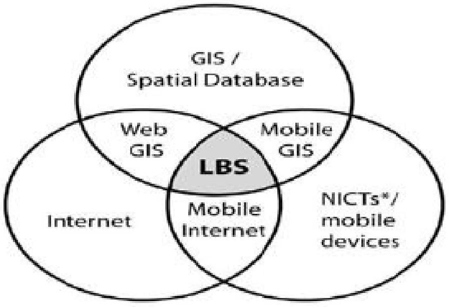
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.

It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.

A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**
b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Althoughefforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver's mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver's mobile number and MMID, and transfer the funds to the receiver's account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to nonexistent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure servers. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone’s screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

Annexure-F (GIGW)

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the ‘State Emblem of India (Prohibition of improper use) Act, 2005’.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:

   i. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India’ (for a Central Government Department).

   ii. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India’ (for a State Government Department).

   iii. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).

   iv. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)’ (for a District of India).

4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the searchengines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.

5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the

Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Uttar Pradesh, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.

b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor's system during the process and what shall be the purpose of the same.

Whenever a Department's website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the “Policy on Open Standards for e-Governance” and “Technical Standards on Interoperability Framework for e-Governance”.

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India” (hereinafter referred to as the “Policy”) will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government’s approach on the use of “Open APIs” to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.

ii. Enable quick and transparent integration with other e-Governance applications and systems.

iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.

iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.

v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.

ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.

iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.

iv. The Government organizations shall make sure that the Open APIs are stable and scalable.

v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.

vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.

vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.

viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.

ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.

x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

Annex-H (Internet of Things)

1. Sensor & Actuators

a. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.

b. Identification Technology

ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

c. Domain Specific Compliance:

Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. Communication Technology

a. Thread:

Networking protocol called Thread that aims to create a standard for communication between connected household devices.

b. AllJoyn:

Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.

c. IEEE 802.15.4:

It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).
IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

d. **IETF IPv6 over Low power WPAN (6LoWPAN):**
It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
6LoWPAN Frame Format
Fragmentation and Reassembly
Header Compression
Support for security mechanisms

e. **IETF "Routing Over Low power and Lossy (ROLL):**
IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)
RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)
RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**
It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. **Use Case/ Application Specific:**

i. **Industrial IoT (IIoT):** Object Modeling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modeling
- Structured Assurance Case Metamodel
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modeling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. Consortia

a. Open Interconnect Consortium:

OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

b. Industrial Internet Consortium:

It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. Architecture Technology

a. IEEE P2413: Standard for an Architectural Framework for the Internet of Things

The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. Further Readings for Standards

a. ITU Standardization Roadmap

This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

b. IERC Position Paper on IoT Standardization:

It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

Annex-I (Smart Parking)

The following standards and certifications need to be followed:

1. **Entry Device**
   i. Communication protocol should be TCP/IP
   ii. Conform ISO 9001 Quality Assurance Standard
   iii. CE, FCC, IC, CNRTLUS certified
   iv. Degree of protection based on IEC 60529: IP43

2. **Exit Device**
   i. Conform ISO 9001 Quality Assurance Standard

3. **Entry/Exit Barrier**
   i. The Barrier unit must conform to ISO 9001 Quality Assurance standards
   ii. CE, Ukr - Sepro certified
   iii. Degree of protection: IP34D

4. **Sensors**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP67

5. **Parking light aisle indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP55

6. **Indoor LED indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP33
   iii. Communications: Bus RS-485

7. **Other Technical Specifications**

Annex-J (Public WI-FI)

1. All equipment must support the following standards/capabilities:

i. 802.11n

ii. 802.11ac

iii. 802.11e Quality of Service (QoS)

iv. WMM Wireless Multimedia Extensions

v. WMM Powersave

vi. 802.11h Dynamic Frequency Selection and Transmit Power Control

vii. 802.11i Security, including AES

viii. 802.1X with dynamic VLAN policies

ix. WPA2-Enterprise certification

x. 802.11r Roaming

xi. preferred: 3X3 MIMO

xii. preferred: Polycom/SpectraLink VIEW Certification, SpectraLink Voice Priority

xiii. preferred: Wi-Fi Certified Voice-Enterprise

2. Wireless Access points specs

i. Shall be IEEE 802.11ac compliant concurrent dual radio access point.

ii. Shall feature a three spatial-stream 802.11ac (3x3 MIMO) integrated or external dual band (2.4GHz & 5GHz) antenna.

iii. Shall have 802.3af or 802.3at compliant Gigabit PoE UTP port and a console port.

iv. Shall be IEEE 802.3af PoE compliant and both the radios shall operate at full power and full performance on 802.3af PoE/Gigabit Ethernet.

v. Shall be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g/n/ac client devices.

vi. Shall support up to 16 SSID/VSC profiles.

vii. Shall support simultaneous detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.

viii. Shall support both centrally managed mode (configured and updated via a controller) and autonomous mode (standalone in the absence of a controller).

ix. Shall support auto-selection of RF channel and transmit power.

x. Shall support enforcement of client authorization based on user credentials (802.1X/EAP), and hardware identifiers (MAC address, WEP key).

xi. Shall support ACS or similar feature to reduce co-channel interference (CCI) by automatically selecting an unoccupied radio channel.

xii. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

xiii. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services

xiv. Must support up to 23dbm of transmit power in both 2.4 GHz and 5 GHz radios.

xv. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

Annex-H (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