

AMRITSAR SMART CITY LIMITED

SCO – 21, 2nd Floor, District Shopping Complex, B-Block, Ranjit Avenue,
Amritsar 143001 | Email: ceoasclsr@gmail.com | Tel: + 91-183-5015048



REQUEST FOR PROPOSAL

For

Selection of Master System Integrator for
Implementation & Maintenance of Smart Solutions
(Phase - I) in Amritsar City

Volume II: Scope of Work

RFP Number: 09/ASCL/2018-19

Issued on 06/12/2018

Table of Contents

Table of Contents	2
1 Existing Solutions.....	6
1.1 City Surveillance.....	6
1.2 Air Quality Sensor	6
1.3 Online Waste-Water Quality Management System.....	6
1.4 Communication Network	7
1.5 Integrated Command Control Centre (ICCC)	7
2 Overall Solution Architecture	9
2.1 Indicative Logical Architecture.....	9
2.2 Indicative DC Solution Architecture	10
3 Scope of Work	11
3.1 General Scope of Work.....	11
3.2 City Surveillance.....	12
3.3 Integrated Command and Control Centre.....	17
3.4 On-premise Data Centre for City Surveillance.....	21
3.5 Disaster Recovery on Public Cloud.....	24
3.6 Communication Network	25
3.7 Public Address system.....	26
3.8 Emergency Call Box with Panic Button.....	26
3.9 Body worn Camera.....	26
3.10 Air Quality Monitoring Stations	26
3.11 Online Waste Water Quality Monitoring System	27
3.12 Variable Message Display (VMD).....	27
3.13 Solution Design, Development, Procurement, Delivery, Configuration, Implementation, Integration, Testing, Commissioning, Operations & Maintenance	27
3.14 Application Maintenance	30
3.15 Application Change & Version Control.....	30
3.16 Problem Identification and Resolution	31
3.17 Provision, deployment and supervision of manpower for Operations & Maintenance of ASCL Smart Solutions.....	31
3.18 Training and Capacity Building.....	31
3.19 Helpdesk.....	32
3.20 Acceptance Testing	32
3.21 Go Live of the project.....	34
3.22 Vendor Management	34
4 Implementation Plan, Payment Schedule and Deliverables	35
5 Annexure I: Functional Requirements Specifications.....	38
5.1 Field Infrastructure Functional Requirements.....	38

5.2	Communication Network	38
5.3	City Surveillance.....	40
5.4	Public Address (PA) System	55
5.5	Emergency Call Box (ECB) System.....	57
5.6	Variable Message Display (VMD).....	58
5.7	Air Quality Monitoring System	61
5.8	Online Water Quality Analyser	62
5.9	Data Centre on Premise	63
5.10	General Requirements of Public Cloud Infrastructure.....	64
5.11	Data Centre on Cloud	69
5.12	Disaster Recovery on Cloud.....	69
5.13	Integrated Command Control Centre	73
6	Annexure II: Technical Specifications Hardware	98
6.1	City Surveillance.....	98
6.2	Environment Sensor	111
6.3	Waste Water Sensor	115
6.4	Network Backbone.....	125
6.5	Variable Message Display (VMD) Board.....	130
6.6	Sewerage Treatment Plant Integration.....	132
6.7	Data Centre.....	133
6.8	Generic IT Hardware	175
6.9	Non - IT Hardware.....	183
6.10	Helpdesk Hardware.....	204
7	Annexure III: Technical Specifications Software.....	208
7.1	Data Centre Platform Software	208
7.2	Antivirus	236
7.3	Data Centre Infrastructure Management Software.....	238
7.4	Air Quality Management Software	245
7.5	Surveillance Software.....	246
7.6	Waste Water Quality Management Software	260
7.7	Helpdesk Software	261
7.8	Variable Message Display Software.....	262
7.9	Sewerage Treatment Plant Integration.....	263
7.10	Business Continuity Management Software	265
8	Appendix V: Indicative locations for Field equipment.....	267
9	Appendix VI: Air Quality Monitoring Station Locations	290
10	Appendix VII: Water Quality Analyzer Locations.....	291
11	Appendix VIII: Indicative Use Cases.....	292
12	Appendix IX: Indicative Layout of ICCC Room	305

13	Appendix X: Existing city surveillance infrastructure.....	306
14	Appendix XI: Existing Ambient Air Quality Stations.....	312

The RFP Document consists of three volumes as listed below and would include any addenda issued in accordance with Clause 5.18 of the Volume I of this RFP.

Volume I	Instructions to Bidders
Volume II	Scope of Work
Volume III	Draft Agreement ("Agreement")

This is Volume II of the RFP document.

1 Existing Solutions

1.1 City Surveillance

Punjab Police, Amritsar City has taken initiative in implementing CCTV surveillance Project in select areas of Amritsar City. Punjab Police is one of the major stakeholder of the City Surveillance Project.

There are 202 cameras (200 Fixed and 2 PTZ) which are currently installed at 40 different locations across the Amritsar City. These cameras are monitored through 6 isolated control centres by Punjab Police. Details of existing CCTV Surveillance cameras installed in Amritsar city is mentioned at Annexure IX: Existing city surveillance infrastructure

The key objective of real-time feeds from all cameras installed at these locations shall be integrated with the ICCC as part of scope of this project. The storage of video shall remain at local monitoring control rooms. The scope of software integration between ICCC and local monitoring stations shall include retrieval of video over the network for analytics and real-time viewing on video wall at ICCC. The MSI shall integrate with existing Video Management and Recording servers for achieving this functionality. Apart from above, the existing infrastructure integration, new surveillance infrastructure shall be installed at locations listed in Annexure: IV

1.2 Air Quality Sensor

The Punjab Pollution Control Board is the key stakeholder responsible for preserving the air, water and other environment laws in State of Punjab. The list of existing Ambient Air Quality Stations in the Amritsar under National Air Monitoring Programme (NAMP) is as given at Appendix XI: Existing Ambient Air Quality Stations

The feeds from existing air quality monitoring stations shall be integrated at the Integrated Command and Control Centre (ICCC) along with installation of Air Quality Monitoring stations at seven (7) new locations in Amritsar City with requisite software at ICCC as part of this project.

1.3 Online Waste-Water Quality Management System

1.3.1 Overview

Amritsar falls under the catchment of Hudhara drain which flows in the north of the city and moves downwards before entering Pakistan. The storm water of the city of Amritsar is carried through following two main drains being maintained by drainage division of Irrigation Department.

- Tung Dhab drain
- City Outfall drain

Primary objective of the Online Water Quality Management System (OWQMS) for drainage canals in Amritsar under the smart city program is to monitor the quality of waste-water in the drainage canals and monitor effluent treatment measures being done in the canal. The project goals shall be to provide the following:

- a. Monitoring of drainage water quality remotely through ICCC
- b. Monitoring the Quality of effluent treated and processing at the inlet and discharge of each drain (Tung Dhab and City Outfall)
- c. Measure waste water quality parameters like BOD, COD, Dissolved Oxygen, TSS, NH₄-N, PH, Temperature and Oil & Grease in Tung Dhab and City Outfall Drain

- d. Provision automated data sharing with State and Central Pollution Control Board websites and databases

1.4 Communication Network

Existing services in Amritsar city include Hybrid Fibre Coaxial Cable TV, Internet services, Cellular services to telecom networks, Enterprise connectivity, Fibre to Home services, Dedicated Leased lines for internet and P2P services, MPLS VPN connectivity etc.

In context of network connectivity for Amritsar Smart City projects, the type of connectivity desired for projects is detailed below:

- Connectivity of Field Junction Boxes for Surveillance project shall be wired backbone with adequate bandwidth meeting requirements of SLA as defined by the project at end-to-end service level.
- Online Waste Water Quality Systems, and Online Air Quality Monitoring Stations shall use cellular backbone for connectivity with adequate bandwidth to meet end-to-end SLAs at each service level

1.5 Integrated Command Control Centre (ICCC)

1.5.1 Overview

Currently Amritsar City does not have a centralized state of the art facility Command and Control facility for Police and Municipal functions in the city.

1.5.2 Existing Infrastructure Details

Level of IT enablement of Emergency Response System in Amritsar City

The Amritsar Police Department: City, Rural and Traffic have static webpage, providing basic information about the department with contact details of the key officials. The list of the information technology interventions available in the Police control room are given below:

Table 1-1 Existing Technology Interventions at Police Control room

S. No.	Features / Facility
1.	Call distribution system
2.	Call incident management system
3.	Vehicle tracking system
4.	Voice Recording
5.	Call takers available
6.	Dispatchers
7.	Standard Operating Procedures

1.5.3 Ambulance Emergency Response System – Dial 108

A centralised call taker and dispatch facility is established in Amritsar for the State of Punjab. A total number of 22 ambulances are allocated for the Amritsar city. These 22 ambulances are stationed at 22 locations earmarked for them. These ambulances are used for carrying of patients to the nearest Public Health Centres or Government Hospitals or transfer of patients to the Postgraduate Institute of Medical Education and Research (PGIMER) in Chandigarh. Currently, these vehicles do not have Mobile device terminal, communication is established using mobile phones. GPS systems are also not available in these vehicles.

1.5.4 Fire Emergency Response Systems

The fire department of Amritsar has 6 fire stations and is under the control of Municipal Corporation, Amritsar. The fire stations are headed by fire brigadiers. Following are the types of vehicles available with the fire department: Fire Trucks, Medium size Trucks, Mini Fire Vans and two-wheelers. The fire department use their mobile phones to communicate with the control room and other fire stations. Also, department has a hot line alarm for critical assets in the city.

Table 1-2 Summary of the IT interventions of police, fire and ambulance control rooms

S. No.	Control Room	Assets/Processes	Level of IT Intervention
1.	Police Control Room: Law & Order (City limits – C-Division)	Call taking	Manual (automated system is not operational)
		Dispatch	Manual (automated system is not operational)
		Vehicles tracking	GPS not available
2.	Police Control Room: Traffic	Call taking & Dispatch are same	Manual records
3.	Ambulance	Call taking	Computerised
		Dispatch	Computerised
		Vehicle tracking	GPS not available
4.	Fire	Call taking	Manual records
		Dispatch	Manual records
		Vehicle tracking	GPS not available

1.5.5 Unified Emergency Response System - Dial 112 in Amritsar

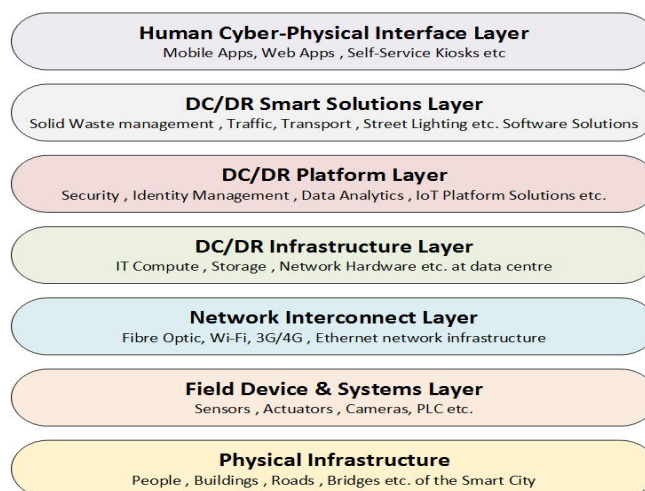
As per the guidelines of the Ministry of Home Affairs, the Government of Punjab is in the process of implementing Dial 112 project in the State. Police Department has been identified as the nodal agency to implement the project across the state. The objective of project is to integrate the Police, Fire, and Ambulance in the State with a single emergency number across the state.

The project shall be implemented by CDAC across the State. A centralised call taker facility with twelve decentralised dispatch centres have been planned across the state. The centralised call centre shall be established in Mohali with 150 seating capacity and 12 dispatch centre across Punjab. An MPLS connectivity shall be used to connect the call taker centre with the 12 dispatch centres. The solutions shall have Geographical Information System (GIS), Computer Aided Dispatch (CAD) system and Mobile Device Terminals. A dispatch centre is being planned for the Amritsar city under Dial 112 project.

The ICCC planned under the Amritsar Smart City shall be exclusively for Video Surveillance and Municipal functions. The ICCC shall implement advanced video surveillance and analytics and integrate with the centralized Dial 112 project planned at the state level for escalating all the incidents detected from video surveillance in the city.

2 Overall Solution Architecture

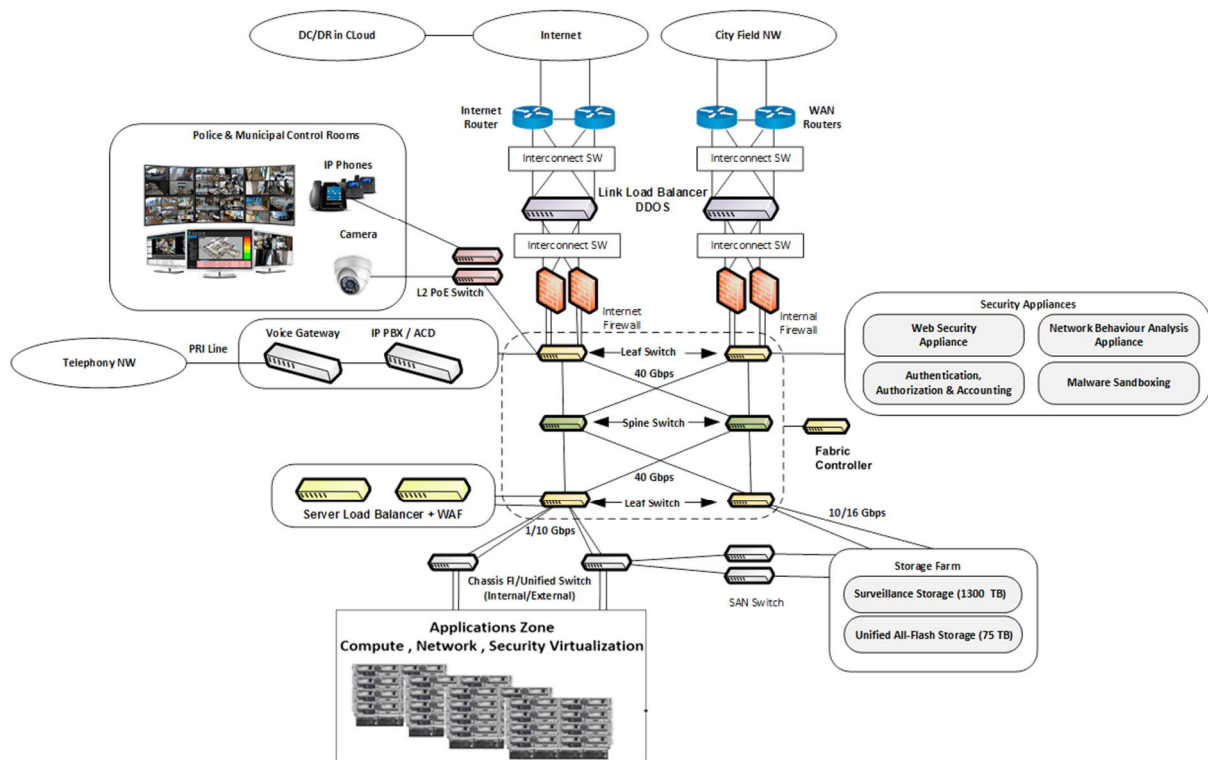
2.1 Indicative Logical Architecture



- Physical Infrastructure of the city comprises of its people, roads, buildings, bridges, parking lots, markets, malls etc. that boost social, cultural and economic growth of the city.
- Field Device & Systems Layer comprises of field devices like environment sensors, surveillance cameras, SCADA systems etc. that control, monitor and safeguard the functions of the city infrastructure at the lowest level.
- Network Interconnect Layer connects all the systems in the field devices and systems layer with each other and with systems in the layers above through wired and wireless networking technologies like Fibre Optics, Wi-Fi, 3G/4G and Ethernet etc.
- Command Centre provides the smart city with a centralized capability to aggregate data from the field devices and systems to a central data centre/control room through the interconnect layer to control and monitor its assets and infrastructure for optimizing operations.
- Command Centre Common Platform provides common platform functionality across all software solutions in the command centre like Security Management, Identity Management, Data Analytics, Unified Database, Internet of Things platforms etc.
- Smart Solutions provides software solutions for multiple functions of the city Municipal Corporations like Solid Waste Management, Traffic Management, Transportation, Security and Surveillance etc. which run in the central Command Centre.

2.2 Indicative DC Solution Architecture

Indicative DC Architecture for Amritsar Smart City



For detailed description of the overall solution, please refer to the functional requirements section.

3 Scope of Work

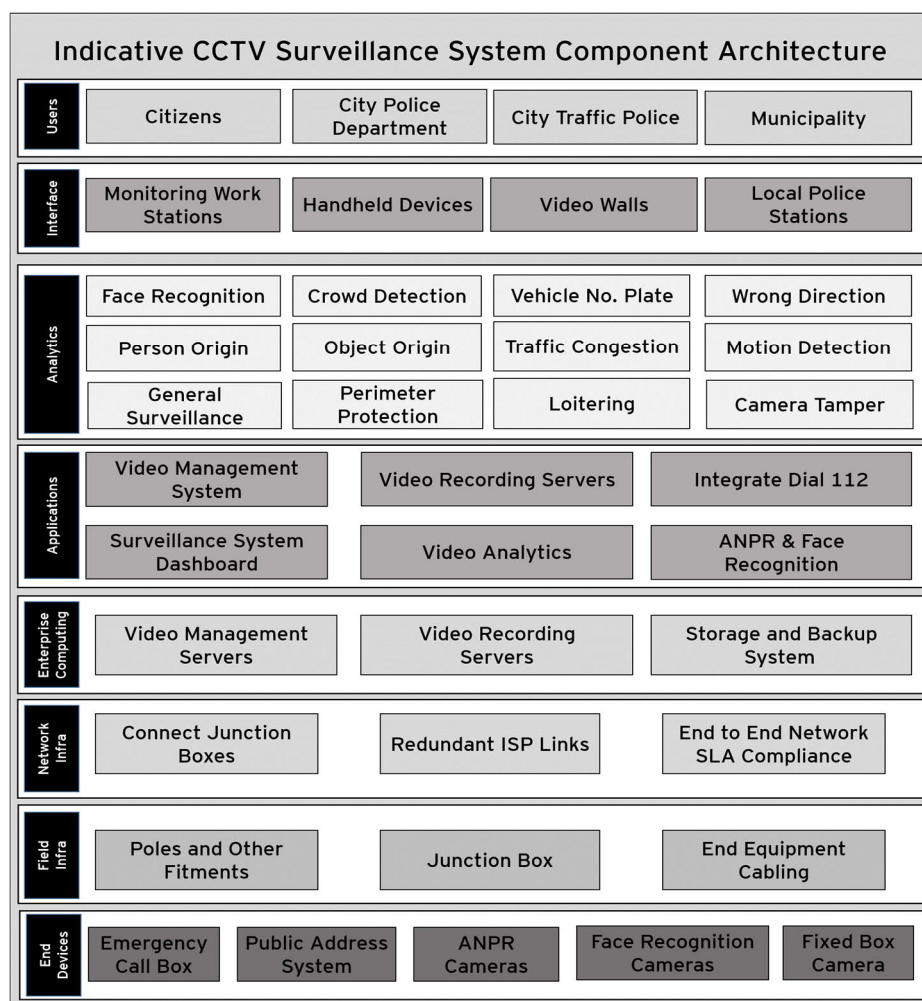
3.1 General Scope of Work

- I. The MSI shall perform detailed site surveys for the purpose of commissioning the field equipment at all the locations under the scope of the Project. The Supply Installation Testing and Commissioning (SITC) shall only commence after the detailed survey report is duly approved by ASCL/ MCA.
- II. The MSI shall identify and obtain necessary No Objection Certificate (NOC), statutory clearances, approvals for erecting the poles, carry out civil work and installing cameras, VMDs, Emergency Call Boxes, Air and Water quality monitoring sensors etc. including provisioning of the required power and network bandwidth.
- III. MSI shall manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees shall be applicable to ASCL for obtaining the necessary permissions. These shall be factored in by the MSI in their Commercial Bid.
- IV. The MSI shall be responsible for the Integration, testing and commissioning of all the IT and non- IT Infrastructure along with all allied equipment, software, updates, patches etc. MSI shall give an undertaking that they will implement all software patches and updates released by OEM to keep performance and security of equipment.
- V. The MSI shall provide all material required for the mounting of components such as Cameras, Air Quality Monitoring Stations with local displays, Water Quality Sensors, Variable Display Board and other field equipment (with all fitments and accessories).
- VI. The MSI shall be responsible to arrange transport of the goods to the project site (s)
- VII. The MSI shall ensure all the equipment's installed in the outdoor locations are vandal resistant
- VIII. The MSI shall provide comprehensive insurance of field equipment for the duration of the contract
- IX. The MSI shall provide training and capacity building for ASCL / Municipal Staff for ICCC software, network and hardware troubleshooting of the systems supplied and installed.
- X. MSI shall implement industry- standard data transports and open protocols
- XI. Periodic preventive maintenance schedules are to be established, executed and shall be duly approved by ASCL.
- XII. A seven (7) day notice shall be submitted to ASCL office for planned maintenance or any scheduled downtime.
- XIII. The MSI shall supply manpower for field operations, ICCC, training and handholding for the project
- XIV. AMC/Warranty should commence from the effective date of go-live. The MSI shall submit Warranty/AMC valid for the duration of the project for all supplied hardware, software, licenses and Non- IT with no extra cost in commercial part of bid. The installation shall be deemed incomplete if any component of the equipment or any documentation/media is not submitted to ASCL. The MSI shall be responsible for the up keep and maintenance of the infrastructure and necessary deliverables under the scope of work during the entire warranty period.
- XV. The MSI shall ensure that all equipment, software and workmanship that form a part of the service are to be under warranty throughout the term of the service contract from the date of service acceptance and commencement. The warranty shall require the MSI to be responsible to bear all cost of parts, labour, field service, pick-up and delivery related to repairs, corrections during the Project Period for any or all such incidental expenses incurred during the warranty period.

- XVI. In case of theft or physically damage the equipment shall be replaced by MSI without any cost implication to ASCL and FIR shall be lodes by the MSI in such cases. In such cases, MSI shall pay for both, material as well as service charges and shall be completely responsible for security of field equipment
- XVII. MSI shall provide Data sheets, User Manual, Training Manual, System manual, troubleshooting guides in original as supplied by the OEM
- XVIII. The MSI shall provide complete technical documentation of hardware, firmware, all subsystems, operating systems, compiler, system software and the other software. The source code of all the bespoke development, APIs, Web services developed for ASCL shall be shared with ASCL. The manuals, wherever applicable shall be in English. All the applicable manuals/documents/Data Sheets for the items delivered and installed should be submitted. Unless and otherwise agreed, the equipment delivered and services rendered shall not be considered as completed for the purpose of go-live until such manuals and drawings have been supplied to the ASCL
- XIX. Before the commencement of User Acceptance Testing, the Master System Integrator shall supply all the operations and maintenance procedures, (together with drawings of the goods and services where applicable)
- XX. The MSI shall provide operations and maintenance of the infrastructure for a period of 4 years from the effective date of Go-Live.
- XXI. The MSI shall manage the Service Levels as per the requirements listed in Volume – III of RFP and provide ASCL with the relevant Software and Automated Tools to monitor the same.
- XXII. The MSI shall furnish the System Generated Service Level reports in the format and frequency as desired by ASCL.
- XXIII. The MSI shall ensure that all IT and Non-IT equipment shall have open interface and protocols for sharing matric relevant to EMS, NMS and BMS systems for monitoring and management of SLAs
- XXIV. The MCA/ASCL shall be responsible for provisioning of the 3-phase power supply and water connection to the MSI. However, running expenses during the contract period on electricity and water supply will be the responsibility of the MSI.
- XXV. MSI shall follow and ensure compliance with the published e-Governance standards, frameworks, policies and guidelines available on <http://egovstandards.gov.in> (updated from time-to-time), Advisories issued by MoHUA for Smart Cities, MeitY etc.

3.2 City Surveillance

Various components of the City Surveillance project, including users of the system are shown in the figure below:



The MSI shall perform survey of all the existing IP Camera locations. There are 6 existing local monitoring centres connected to 40 Camera locations. The MSI shall connect these existing local monitoring centres with the proposed Integrated Command and Control Centre.

3.2.1 Installation of Standard and Cantilever GI Poles

- I. MSI shall provide structural calculations and drawings for the approval of ASCL before commencing installation
- II. MSI shall coordinate with concerned authorities/municipalities for installation of poles
- III. Poles and cabinet shall be so designed that all elements of the field equipment shall be installed, maintained and repaired
- IV. The MSI shall be responsible for preparation of concrete foundation for Galvanized Poles & Cantilevers Poles
- V. MSI shall ensure that physical look of the installation area is restored to its original state after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed
- VI. Carry out SITC of IP Cameras, PTZ Cameras, Public Address System (PAS), Variable Message Signboards (VMS) etc. including appropriate poles & cantilevers and any supporting structures, foundations etc. The designs of the poles shall be approved by ASCL and AMC before installation starts and that necessary design changes incorporated after reviews

- VII. The MSI shall use existing poles in Amritsar City for installing cameras wherever feasible. The quantity of poles as mentioned in RFP BOM is indicative and may vary after detailed site survey. Any additional required poles shall be procured by ASCL on unit rates quoted by MSI after mutual discussion
- VIII. MSI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of cameras shall be made to prevent birds from sitting on top of camera box
- IX. The poles shall be installed by MSI with base plate, pole door, pole distributor block and cover.
- X. The poles installed by MSI shall have proper grounding, earthing and bonding as per relevant standards (to be specified by MSI) for such structures
- XI. Base frames and screws shall be delivered along with poles and installed by the MSI
- XII. In case the cameras need to be installed beside or above the signal heads, suitable stainless-steel extensions for poles need to be provided and installed by the MSI so that there is clear line of sight
- XIII. MSI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles/cantilevers for IP cameras, Variable Messaging Sign boards (for Air Quality Monitoring Station displays) and other equipment
- XIV. MSI shall follow Punjab Roads & Bridges Development Board and other Punjab Government rules and guidelines for the installation of poles

3.2.2 Outdoor Cabinets / Junction Boxes

- I. MSI shall ensure that each location shall be fitted with outdoor cabinets sized and dimensioned to host all equipment necessary to operate Surveillance and future Traffic management and enforcement Systems as defined in this RFP. The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby
- II. MSI shall ensure that boxes shall be dustproof and impermeable to splash-water. They shall be suitable for outdoor environmental conditions in Amritsar. They shall have separate lockable doors for:
 - a. Power cabinet: This cabinet shall house the electricity meter, rectifier, battery bank and the power supply system
 - b. Control cabinet: This cabinet shall house the electronic components required for all the field components (Surveillance Cameras, ANPR Cameras, Face Recognition Cameras, Public Address Systems, Traffic Detection and Management Systems etc.) at that location. The typical end equipment housed in the junction box shall include e.g. ANPR LPU, Face Recognition LPU, PA External Amplifiers, Intelligent Traffic Light Controllers, and Industrial Grade Ethernet to Fibre Optic Switches etc.
- III. MSI shall ensure that internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power, marked with identifiers and installed in proper cable guidance trays
- IV. The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
- V. The MSI shall ensure that all Junction Box enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters for temperature and humidity control that shall not require maintenance and shall allow free circulation of air

inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation

- VI. MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Amritsar City throughout the year
- VII. MSI shall ensure that heavy electrical load shall be directly powered in Junction Box without Battery Backup. E.g. Variable Message Display

3.2.3 Civil and Electrical Works

Between Network Service Provider and Junction Box:

- I. The MSI shall be responsible for carrying out all the civil work required for setting up all the field components of the system
- II. The MSI shall be responsible for preparation of Chambers with metal cover at every junction box, pole and at road crossings
- III. The MSI shall be responsible for Concrete foundation from the Ground for outdoor racks
- IV. The MSI shall place route marker as per given alignment & maintaining offset distance from road centre as per norms set by concerned government authorities
- V. The MSI shall use barricading and signage board as per Requirements of concerned Government authority pertaining to specific roads
- VI. The MSI shall coordinate with the existing utility owners before starting the excavation work. If required, the MSI shall ensure the presence of representative of existing utility owners.
- VII. Once the utilities have been located, MSI shall physically identify the exact location of the utilities by taking test pits of minimum width of 2 meters across the drill path, to determine the actual location and path of any underground utilities. MSI shall not commence boring operations until the location of all underground utilities within the work area have been verified.
- VIII. The MSI shall dispose the surplus earth material to a suitable location as indicated by concerned Government authorities
- IX. The MSI shall backfill and reinstate the area to its original condition as per the guidelines issued by the concerned government authorities pertaining to specific road after completion of work.
- X. MSI shall carry out all the electrical work required for powering all the components of the System.
- XI. Electrical installation and wiring shall conform to the applicable National Electrical Code 2011.
- XII. The recurring expenses towards diesel and electricity would be reimbursed to the MSI on actual basis on a quarterly basis

Between Junction Box and CCTV Locations:

- I. MSI shall be responsible for carrying out all the civil work required for setting up all the field components of the system
- II. MSI shall be responsible for preparation of concrete foundation for Galvanized Poles & Cantilevers Poles
- III. MSI shall use GI pipe along with DWC pipe for protection if depth of cable is less than 6 inches as digging is not possible up-to prescribed depth due to Utility under earth or Rocky soil.
- IV. Power and Data Cable shall be laid in separate conduits / ducts and separated by minimum 6" distance

- V. Outdoor-rated Unshielded Twisted Pair (UTP) Communications Category (CAT) 6 Cable with armouring to provide Ethernet connectivity between network switches and end devices such as CCTV located within 100 meters from the switch location.
- VI. Each conductor of the UTP cable shall be insulated with a coloured high density polyethylene jacket with varying twisted length to minimize crosstalk.
- VII. The termination shall protect the cable terminations from water and mechanical damage and shall be resistant to salt corrosion.
- VIII. The MSI shall place route marker as per given alignment & maintaining offset distance from road centre as per norms set by concerned government authorities
- IX. The MSI shall use barricading and signage board as per requirements of concerned city administration pertaining to specific roads.
- X. The MSI shall coordinate with the existing utility owners before starting the excavation work. If required the MSI shall ensure the presence of representative of existing utility owners.
- XI. Concreting shall be used to provide additional protection on bridges, culverts and on stretches wherever depth of excavation is less than 0.2Mtr.
- XII. The MSI shall dispose the surplus earth material to a suitable location as indicated by concerned Government authorities
- XIII. The MSI shall backfill and reinstate the area to its original condition as per the guidelines issued by the concerned government authorities pertaining to specific road after completion of work.
- XIV. Electrical installation and wiring shall conform to the electrical codes of India
- XV. MSI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via Junction Box, housing the power supply, with minimum backup as defined in this RFP
- XVI. For the wired cameras, MSI shall provision for drawing power through PoE/POE+ (Power over Ethernet) as primary method and shall use dedicated power cable laid separately along with STP/SFTP cable only in exclusive cases, in case POE/POE+ is not possible

3.2.4 Grounding, Earthing, Bonding and Surge Protection Measures

- I. MSI shall comply with the technical specifications and IS 3043: 1987 taking into account all grounding, earthing, bonding and surge protection measures for system enclosure, equipment, power and signal cabling
- II. MSI shall describe the planned Grounding, Earthing, Bonding and Surge Protection in their technical bid
- III. MSI shall install surge protection devices of adequate capacity for protection of all equipment
- IV. MSI shall install for all interfaces of electronic equipment high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chips due to electrical surges
- V. MSI shall install the chemical Earthing for the equipment that shall meet the related industry standards
- VI. The Earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof

3.2.5 IP Camera Surveillance

- I. MSI shall describe in detail the design, operational and physical requirements of the proposed IP Camera Surveillance system, to demonstrate compliance with all the specified requirements in this RFP
- II. The MSI shall install IP Camera based surveillance system at locations given in Annexure IV: Indicative locations for Field equipment

- III. The MSI shall provide end to end connectivity from all locations to Data Centre
- IV. The MSI shall be responsible to provide Monitoring / Managing Software which shall be required to monitor/ manage the Leased network
- V. Any addition in the number of locations shall need to be connected as per the agreed terms and conditions for already connected sites. Same terms and conditions shall be applicable for change or removal of any site from earlier selected sites

3.2.6 Fault Restoration Services

- I. The MSI shall have field maintenance team to ensure SLA adherence. The Maintenance teams shall comprise of manpower, logistics, required tools/tackles/machinery & equipment etc.
- II. The MSI shall be required to carry out maintenance activities which include identification of fault/cut on ground, obtaining permission from local authorities if required, excavation of earth to expose cable, laying of required length of cable with protection wherever required, installation of Jointing pit & back filling of pit with sand, supply and installation of cable Route Markers and Joint Markers as per specifications
- III. MSI shall observe all national and local laws, ordinances, rules and regulations and requirements pertaining to the work and shall be responsible for extra costs arising from violations of the same

3.3 Integrated Command and Control Centre

The Integrated Command and Control Centre (ICCC) shall function as a common facility for MCA and Police functions. The ICCC shall be used by these agencies to monitor their respective functions and responsibilities.

ICCC shall be the 'nerve Centre' of Amritsar that assists in enhancing efficiencies of the City Operations, Management and Security. It provides a holistic view of all city operations allowing monitoring, control and automation of various functionalities at an individual system level along with enabling cross-system analytics. The ICCC shall be deployed in Amritsar as part of this project, to make the city operations intelligent, integrated and efficient.

The scope of work of MSI for the ICCC shall include:

- I. The MSI shall design, supply, install and commission ICCC Platform in accordance with the Functional & Technical requirements listed in Annexure I: Functional Requirements Specifications and Annexure II: Technical Specifications Hardware
- II. MSI shall manage the ICCC facility on 365 X 24 X 7 basis
- III. The MSI shall deliver a roll out strategy for implementing and integrating the smart solutions of the city utilities and surveillance in the ICCC
- IV. MSI shall implement, monitor and manage the security policies and procedures for the IT as per ISO 27001 standards and ITIL and NON- IT assets as per the leading industry practices
- V. MSI shall prepare and implement Standard Operating Procedures (SOP) for the ICCC Platform in consultation with ASCL, MCA and Punjab Police Department
- VI. MSI shall ensure inter-operability, seamless integration and data sharing of data between various solutions by building required APIs between end solutions and ICCC Software Platform. These shall include all sub-systems in this RFP and future solutions (specifically

- Adaptive Traffic Signalling Systems and Solid Waste Management System) to be rolled out by the smart city during contract period of the MSI
- VII. MSI shall share report of various data using reporting tools and visualisation tools as per the requirements of ASCL, MCA and other law enforcement agencies
 - VIII. MSI shall deploy prescriptive and predictive analytics where ever applicable as per the requirements of ASCL
 - IX. MSI shall supply the necessary communication equipment, IP telephony and other necessary infrastructure for the municipal and police department staff to be deployed in the ICCC
 - X. The MSI shall ensure that the overall work shall be in reference to standards published as per ISO 37120 and World Council of City Data (WCCD)

3.3.1 Setting up ICCC

3.3.1.1. Survey and Site Preparation for ICCC and its Data Centre

- I. The MSI shall survey the identified site at MCA office on 2nd Floor, and submit necessary designs such as (but not limited to) for civil, interior, electrical, networking, cooling and fire safety designs for approval from ASCL.
- II. MSI shall carry out assessment of the load bearing capacity of the DC site and propose retrofitting measures required to meet the load requirements of IT and Non- IT equipment's.
- III. ASCL shall carry out a detail of the review of design solution and review design for DC including all its components such as Server Room, operators seating arrangement, office space, supervisors seating arrangement, visitors' gallery, reception area etc. on the parameters of overall Design, Safety & Security and aesthetics and reserves it right to accept, reject or suggest for modifications on the proposed solution. MSI may also deploy services of a professional architect to prepare the interior design of the DC premises and carry out the civil / electrical / furniture work
- IV. The site preparation activity to be carried out by the MSI would include but not limited to civil work for building interiors, realignment of available space based on requirement and architectural plan, necessary masonry, electrical, carpentry and other works, partitioning, flooring, false ceiling & false flooring as appropriately required, painting work, fire proofing of surfaces, cabling, ducting etc.
- V. MSI shall be responsible for the overall architectural design, aesthetic considerations, and optimal utilization of allotted space to ensure that the DC location is state-of-the-art facilities in line with the importance of the ASCL project. If any of the requirements are not mentioned in the RFP, MSI should include the same as part of additional/proposal line items to ensure that the requirements and expectations of ASCL are met
- VI. Upon approval, MSI shall complete the necessary civil, electrical, cooling and interior work.
- VII. The illustrative layout of proposed ICCC is given in Annexure VIII: Indicative Layout of ICCC Room

3.3.1.2. Delivery

- I. The MSI shall inform the ASCL and other required stakeholders about the delivery of items in writing at least 7 days in advance. A copy of the delivery challan should be available along with the delivered items. Upon delivery of the items, a copy of the delivery challan shall be made available to the ASCL for verification and record purpose. A delivery report shall be submitted to the office of ASCL

- II. ASCL/ MCA shall not be held responsible for any damage and theft of the equipment delivered at the installation site

3.3.1.3. Installation and Commissioning

The MSI is responsible for all unpacking, assembling, wiring, installations, cabling, interconnection and commissioning of the delivered components. The installation and testing shall include the following but not limited to:

- I. Installation and commissioning of line items as per the Technical solution design
- II. Upon completion of the installation, Installation certification shall be submitted to the ASCL.
- III. Completion of installation does not mean the Go-live date of the project. The AMC and warranty of the product shall start from the date of Go-live of the project
- IV. The installation document should contain Physical layouts, Electrical layouts, Civil Architectures, Network Drawings as per applicable TIA standards.

3.3.1.4. Facility Management Services

The MSI shall carry out the Facility Management Services on a 365 X 24x7 basis towards Electrical systems, DG, UPS, HVAC & Control systems to meet the SLA, specifications of each component. Operations and Management Manuals as per ISO 2000 standards shall be submitted to the ASCL before the commencement of the User Acceptance Testing. Facility Management Services shall be carried out as per Operation & Maintenance Manual. ASCL reserves the right to amend the manual as per requirement during the course of the operations.

The scope of the FMS services shall include the following but not limited to:

- I. The site interiors, Building Management Systems including all support infrastructure for normal Data Centre operations
- II. The House-keeping activities such as drinking water, waste disposal, cleaning etc. shall be managed by the MSI

3.3.1.5. ICCC Operations and Maintenance activities

MSI shall be responsible for the following maintenance activities but not limited to:

- I. Preventive and corrective maintenance of electrical Systems by licensed electricians
- II. Payment of Electricity charges of project site, which shall be further reimbursed by ASCL on an actual basis
- III. Upkeep of all fittings and furniture which are not limited to chairs, tables, walls plastering, paintings, floorings, glass panels, wall or glass partitions, false ceiling, lights, switches, should be kept intact as in good working conditions
- IV. Preventive and corrective maintenance of UPS, DG sets, accessories and Battery Banks, Access Control, BMS, Fire Suppression System etc.
- V. Spares consumables for PAC, Centralised AC, Comfort AC
- VI. Fuel stock for DG operations

3.3.1.6. Other Infrastructure Management services

- I. Visitor access register shall be maintained. Prior written approval is required for entry of any visitors into the ICCC/Project site
- II. Movement Register shall be maintained. 365 X 24 X 7 access log for a complete record of any person moving in and out of the project site

- III. Maintenance of Access card level security for various parts of the ICCC, server area and other area for various users should be suitably managed by the MSI
- IV. Access to the farm area is to be highly restricted and only authorised technical personnel are to be allowed. Biometric access shall be maintained for the farm area
- V. A separate visitor's log book is to be maintained for the server farm area/Telecom Room where occasional visitors shall be requested to sign in
- VI. The MSI expected to adhere environmental, health, security and safety practices. ASCL shall be not be responsible to the implications of any unhealthy practice or damage caused by the MSI

3.3.2 ICCC Platform

- I. MSI shall design, deploy, install, test and maintain the ICCC Software platform application that integrates various smart city applications as listed below:
 - a. IP Camera Surveillance System
 - b. Variable Message Signboards
 - c. Online Air Quality Monitoring Systems
 - d. Online Waste Water Quality Monitoring System
 - e. Public Announcement Systems
 - f. Emergency Call Box
- II. Smart city application to be integrated by MSI in ICCC for forthcoming phases shall include;
 - a. Solid waste management system
 - b. SCADA of water, gas and electricity utility networks
 - c. Smart Parking
 - d. Intelligent Street Lighting
 - e. Intelligent Traffic Management System
 - f. Solar Grids
 - g. Other applications as identified by ASCL and MCA
- III. MSI shall be responsible to provide any hardware, software, services required to integrate, control and monitor any future application, including but not limited to applications stated above, with deployed ICCC during the contract duration at no addition commercial implications to Purchaser.
- IV. MSI shall ensure complete data integration along with control, monitoring and provisioning of IoT sensors and end equipment is possible from ICCC Software platform and provision for all the above integration as part of their proposal submission.
- V. MSI shall ensure the transfer of feeds to other Police control centres, Government Departments and offices and mobile devices of staff as per the application requirements

3.3.3 Integration of ICCC with Dial 112 project

The control rooms of Police, Ambulance and fire department are planned to be integrated under single system call Dial 112. The dial 112 shall be the universal number for all the emergency services. In Punjab, the Dial 112 is planned to be implemented in distributed model. In this model, there shall be a centralised call taker centre and 12 dispatch centres across 12 districts. The police patrol vehicles, ambulance and fire vehicles can be dispatched from these dispatch centres. It is envisaged that MSI shall develop functionality to re-direct the incidents generated by CCTV surveillance, Emergency Call Box system to Dial 112 system seamlessly based on the rules and conditions defined.

3.4 On-premise Data Centre for City Surveillance

The broad scope of work for MSI for Data Centre is as below:

- I. Design, Installation, Testing and Commissioning of the Data Centre at 2nd Floor of MCA office, which will be used to host Applications and Data for City Surveillance Project
- II. The MSI shall deploy, install, configure and customize necessary Software solutions, as mentioned in the relevant sections of this RFP
- III. MSI shall ensure surveillance video feeds will be stored in the local Data Centre for 30 days. After which indecent specific feed / triggers will only be saved on unified storage
- IV. Data Centre shall confirm to Tier III standards except for the Power redundancy limitation due to single supply from the PSPCL substation.
- V. The MSI shall use virtualization technologies to be used to reduce the physical space required for hosting
- VI. Data Centre should be as per Telecommunications Infrastructure Standard for Data Centre and should be Certified 27001.
- VII. The MSI shall ensure that access to the Data Centre Space and physical access to the place would be given only to the authorized personnel.
- VIII. The MSI shall install Indoor CCTV Cameras to monitor the physical access of the system from remote location
- IX. The MSI shall ensure Physical Access to the building hosting Data Centre should be access controlled and security personnel shall be deployed 24x7 at all entry and exit points
- X. 24x7 monitoring & management of availability & IT security of the infrastructure & assets (including data, servers, systems etc.) through the Enterprise Management Solution implemented for Project shall be the responsibility of Master System Integrator
- XI. Perform patch management, testing and installation of software upgrades issued by the OEM/ vendors from time to time. These patches/ upgrades, before being applied on the live/ production environment, shall be tested as per the Patch management and release procedures. Any downtime caused due to up gradation & patches shall be to the account of the MSI and it shall not be considered as 'Agreed Service Downtime'.
- XII. Develop the Standard Operating Procedures (SOPs), in accordance with the ISO 27001 & ITIL standards, for Data Centre Operations and Management. These SOPs shall cover all the aspects including Infrastructure installation, monitoring, management, data backup & restoration, security policy, business continuity & disaster recovery, operational procedures etc. The MSI shall obtain sign-offs on the SOPs from the ASCL and shall make necessary changes, on a half yearly basis, to the fullest satisfaction of ASCL
- XIII. Preventive maintenance, carrying out the necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours of the ASCL, unless inevitable and approved by the ASCL
- XIV. Reactive maintenance that is intended to troubleshoot the system with sufficient teams
- XV. Performance tuning of system as may be needed to comply with SLA on continuous basis
- XVI. Monitor and record, server & database performance and take corrective actions to ensure performance optimization daily
- XVII. System administration tasks such as managing the access control system, creating and managing users, taking backups etc.

- XVIII. Produce and maintain system audit logs on the system for a period agreed to with the ASCL.
- XIX. Review security advisories (such as bulletins generally available in the industry) on a regular basis to determine vulnerabilities relevant to the information assets and take necessary preventive steps

Note: The MSI shall ensure that all the licenses of proposed application / system software etc. procured for this project are procured in the name of Amritsar Smart City Limited (ASCL)

3.4.1 Setting up Network Operations Centre (NOC)

- I. MSI shall setup NOC in the ICCC to monitor and control the DC operations for the entire project
- II. The NOC shall analyse network problems, perform troubleshooting etc. The key objective of the NOC is to ensure the health and availability of components and services.
- III. When necessary, NOC shall escalate problems to the appropriate stakeholders. For emergency conditions, such as a power failure of the NOC, procedures shall be in place to immediately contact technicians to remedy the problem
- IV. All the IT devices that are installed by the MSI shall be Simple Network Management Protocol ('SNMP') enabled and the MSI shall centrally and remotely monitor and manage the devices on a 24x7x365 basis. It should also be provisioned to bring Non-IT components on the common monitoring
- V. MSI to establish and implement leading practices of IT service Management like Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO)/IEC 20000 standard that shall promote the adoption of an integrated approach to effectively deliver managed services to meet the requirements.
- VI. MSI shall identify all assets and document the importance of these assets. The asset inventory shall include all the information necessary to recover from a disaster, including type of assets, format, location, backup information, license information etc.
- VII. MSI shall undertake scheduled and ad hoc maintenance (on need basis) and operations like configuration backup, patch management and upgrades
- VIII. MSI shall establish basic tools for IT and Non-IT management to undertake health check monitoring, troubleshooting etc. for all Network operations
- IX. MSI shall establish access control mechanism and shift wise attendance management system
- X. The MSI shall ensure that all resident engineers in the NOC are certified (of the OEMs of the network components) and are provided at Command and Control Centre for 24/7 operations.
- XI. Security Administration and Management Services:
 - a. Management of security environment of the entire network infrastructure to maintain performance at optimum levels.
 - b. Address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, and vulnerability protection through implementation of proper patches and rules.
 - c. Maintain an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, security solutions, network solutions, etc.
 - d. Ensure that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

- e. Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
 - f. Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, firewalls, servers, desktops from viruses.
 - g. Operating system hardening through appropriate configuration and patch updates on a regular basis.
- XII. Physical & Environmental Security at locations
- a. Ensure that all network switches are secured and are enabled only when required by authorized employees.
 - b. Perform reactive and preventive maintenance exercise
 - c. Monitor the environmental controls for security of network equipment, cabling security and IT hardware management.
 - d. Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001, BS 7799 and BS 15000 guidelines
- XIII. The MSI shall develop Services catalogue for NOC and get a sign off from ASCL.
- XIV. Primary responsibilities of NOC personnel shall include but not limited to:
- a. Network Supervision and Monitoring: Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
 - b. Configuration Management: Ensure the proper configuration of network, systems and applications or the provision of reliable and high-quality end-user services
 - c. Change Management, Network Extension: Ensure efficient day-to-day management of short-term network changes and optimization, including their implementation. This activity shall be synchronized with the maintenance scheduled activities
 - d. Performance Management: Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
 - e. Service and Network Provisioning: Define all necessary actions to be performed when a request for a new service is issued, and control the actions performed at NOC level or field level until completion
 - f. Scheduled Activities Planning: Provide regular plans for all scheduled activities, including preventive maintenance. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities
 - g. IT and DB Management: Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
 - h. Security Management: Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
 - i. Quality Management: Define quality management policies, and ensure implementation and usage for competitive quality of service
 - j. Workforce Management: Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan

- k. Inventory Management: Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- l. Asset Inventory Management: Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
- m. Repair and Return: Receive and repair defective boards, return repaired or replacement boards.

3.5 Disaster Recovery on Public Cloud

Disaster Recovery setup shall be hosted on MeitY empanelled Cloud Service Provider. The hosting approach is given below:

- I. The on-premise data centre functions should fail-over to the cloud in case of DR except video analytics. Design the DR according to RTO/RPO as mentioned below:

Recovery Point Objective (RPO)	4 Hours
Recovery Time Objective (RTO)	1 Hour

- II. DR shall be implemented based on managed cloud services and shall adhere to guideline issued by MeitY over time to time. Service Level for DR shall be as per MeitY guidelines.
- III. The cameras shall operate at lower settings i.e. 720P @ 10 FPS in case of DR scenario. This setting profile shall be applied by VMS on cloud on field cameras to reduce bitrate in DR scenario. ANPR cameras shall operate at 720P @ 25 FPS.
- IV. The video recording storage used on cloud shall be released after the Disaster/Disruption period has ended and only flagged data shall be retained and synced back to on premise data centre after it resumes the normal operations
- V. Viewing bandwidth shall be provisioned for minimum of 5% cameras streams at one time in DR scenario. During the period of disaster, it shall be possible to view video feeds from multiple police viewing centres in the city.
- VI. All the important video evidence shall be moved to unified all flash storage on regular basis with help police personnel (ideally within 7 days).
- VII. The complete application databases, tagged video evidence data and other important data and files on 75 TB unified storage shall be replicated in cloud on based on RPO/RTO guidelines.
- VIII. Video Analytics & face recognition shall not be operational on DR.
- IX. ANPR shall be functional during DR period.
- X. The camera stream to DR shall be activated only in DR Scenario to reduce bandwidth cost.
- XI. There should be sufficient capacity (compute, network and storage capacity offered) available for near real-time performance (as per the Service Level requirement of the ASCL) during any unanticipated spikes in the user load.
- XII. Cloud services should be accessible via internet and from control rooms
- XIII. ICCS platform and Surveillance & Security applications and their backend shall be hosted on premise Data Centre in Amritsar.
- XIV. DC Cloud Compute Instances for IoT Applications shall run 24 X 365. These should be sized optimally for current requirements of end device, processing and storage.
- XV. IoT field devices data such as Air Quality, Water Sensor etc. should be retained for the last 5 years.
- XVI. DR on cloud instances shall be configured in pilot light mode with only necessary machines running 24 X 365 mode. All remaining compute instances shall be started on need basis and billed as per the usage.

- XVII. Total sizing period for the DR shall not exceed 24 days a year. Sizing for single continuous DR operation shall not be more than 7 days from video storage perspective.
- XVIII. Video data stored on Cloud shall be deleted after 7 days after taking appropriate backup of critical video footage data to cloud storage.
- XIX. The cloud backup video files and application databases shall be brought in sync with unified storage in DC after DC restoration.
- XX. Connectivity from DC to DR shall use a VPN tunnel over the underlying network connectivity.

3.6 Communication Network

3.6.1 General Guidelines

ASCL intends to have Leased Network Backbone which can support all the current planned initiatives i.e. City Surveillance, Smart Parking, Air Quality Monitoring Stations, Integrated Command & Control Centre & Data Centre, Variable Message Display etc. and scalable to accommodate future IT requirements of the city.

- I. Critical network design parameters such as security, reliability, scalability, manageability, interoperability and resiliency in end-to-end service oriented network delivery shall be considered when taking network backbone on lease across the city from existing service providers.
- II. MSI shall arrange for the Right of Way for any new network laying / installation of RF Towers and Radio Antennas that is to be installed as part of smart city initiative and for sole usage of smart city applications. ASCL shall help in providing ROW permissions by coordinating with AMC.
- III. In case of installation of RF Towers and Radio / Antennas on any private property for Network Backbone, MSI shall arrange ROW permissions on his own.
- IV. The network backbone is expected to provide a converged network, bringing together different city management vertical solutions on a common network infrastructure for Amritsar. The converged network shall facilitate information exchange between resources and applications across different domains.
- V. The network architecture proposed shall comply with the SLA's, best practices and industry standards to ensure high availability, scalability, manageability and security for the information, services and solutions being managed on the network.

3.6.2 Leasing of Network

- I. The MSI shall take services of Network Service Provider on lease basis with sufficient capacity for the entire duration of the contract
- II. The MSI shall provide network connectivity at all required locations as mentioned in the Annexure IV: Indicative locations for Field equipment
- III. The MSI shall provide end to end connectivity from all locations to Data Centre
- IV. The MSI shall be responsible to provide Monitoring / Managing Software which shall be required to monitor/ manage the Leased network
- V. Any addition in the number of locations shall need to be connected as per the agreed terms and conditions for already connected sites. Same terms and conditions shall be applicable for change or removal of any site from earlier selected sites

3.6.3 Fault Restoration Services

- IV. The MSI shall have field maintenance team to ensure SLA adherence. The Maintenance teams shall comprise of manpower, logistics, required tools/tackles/machinery & equipment etc.
- V. The MSI shall be required to carry out maintenance activities which include identification of fault/cut on ground, obtaining permission from local authorities if required, excavation of earth to expose cable, laying of required length of cable with protection wherever required, installation of Jointing pit & back filling of pit with sand, supply and installation of cable Route Markers and Joint Markers as per specifications
- VI. MSI shall observe all national and local laws, ordinances, rules and regulations and requirements pertaining to the work and shall be responsible for extra costs arising from violations of the same

3.7 Public Address system

- I. The MSI shall install IP based Public Address System at the locations in the city as mentioned in Annexure IV: Indicative locations for Field equipment
- II. 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 room
- III. The PA system software installed by MSI at ICCC 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. The system shall also be able deliver pre-recorded messages to the loud speakers attached to them over the IP network and locally attached media for public announcements
- IV. MSI shall ensure that the system shall contain an IP based amplifier and uses PoE/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)

3.8 Emergency Call Box with Panic Button

- I. The MSI shall SITC Emergency Call Box/Panic buttons at locations listed in
 -
 - Variable Message Sign boards along with all the required Poles, Gantry structure shall be installed as per the technical specification in the RFP

3.9 Body worn Camera

- I. The MSI shall supply body camera equipment, accessories and ensure all services required to fully implement body cameras. Initial deployment is anticipated to consist of camera systems to outfit approximately 50 cameras.
- II. The MSI proposed solution shall include accessories, software application(s), add-ons, required for successful implementation of body cameras solution.

3.10 Air Quality Monitoring Stations

- I. MSI shall install the Air Quality monitoring stations and local displays at identified locations as per Annexure V: Air Quality Monitoring Station Locations

- II. MSI shall integrate the Air Quality Monitoring stations with the ICCC to capture and display/ provide feed on the above-mentioned air quality parameters at website / portal / mobile application
- III. The MSI shall also integrate with the existing and new sensor data with ICCC and State Pollution Control board through web, mobile and API interfaces
- IV. MSI shall relay the Information instantaneously to digital signage installed alongside the Air Quality Monitoring stations to display prevalent air quality conditions

3.11 Online Waste Water Quality Monitoring System

- I. MSI shall undertake SITC of Online Waste Water Quality Monitoring Stations at the Tung Dhab and City Outfall Drainage Canals
- II. Online Waste Water Quality Monitoring Station (OWQMS) shall measure the parameters listed in Functional Requirements using Intelligent Edge Gateways integrated with probe analysers. The OWQMS system shall be continuously monitoring the parameters at the Tung Dhab and City out fall drain
- III. MSI shall be responsible for data transmission and integration of OWQMS system hosted in Public Cloud using open SCADA/IoT communication protocols
- IV. The MSI shall integrate the OWQMS software with ICCC software over REST/Stream interfaces and provide dashboards as per requirements of this RFP and ASCL
- V. The MSI shall be responsible for securing the field infrastructure like electrical panels and floating in-situ buoys with probes using protective fencing and chains anchoring the buoys to the embankment respectively

3.12 Variable Message Display (VMD)

- MSI shall undertake SITC of VMD boards shall be designed, supplied, installed and commissioned at designated number of locations as per Annexure IV: Indicative locations for Field equipment
- Variable Message Sign boards along with all the required Poles, Gantry structure shall be installed as per the technical specification in the RFP

3.13 Solution Design, Development, Procurement, Delivery, Configuration, Implementation, Integration, Testing, Commissioning, Operations & Maintenance

a. Systems Requirement Study & Solution Design

Solution Study

- I. The MSI shall perform the detailed assessment of the functional requirements for the services
- II. MSI shall prepare the Functional Requirement Specifications (FRS) & System Requirement Specifications (SRS) provided therein, based on their individual assessment, and in consultation with ASCL and its representatives
- III. FRS and SRS prepared by the MSI shall be submitted to ASCL for inputs/ suggestions and same shall be incorporated by Master System Integrator
- IV. A formal sign-off shall be provided by ASCL

Solution Design

- I. The MSI shall design integrated solution architecture for meeting the System Requirement Specifications and submit to ASCL. The solution design should have seamless integration of all the components comprising of the solution being designed. The solution design shall include, but shall not be limited to application architecture, user interface, database structures, security architecture, network architecture, DC & DR architecture etc.
- II. MSI shall be responsible for ensuring the compliance of the end product to the requirements specified by ASCL in the RFP

Development/ Configuration / Work Around for ASCL Smart Solutions

- I. The MSI shall perform the Development/ Configuration/ Work around of ASCL Smart Solutions based on the requirements/ specifications approved by ASCL

Solution Testing

- I. The MSI shall design the Testing strategy including traceability matrix, test cases and conduct testing of various components of the software developed/ configured for the Project
- II. The software testing shall include but not limited to Unit Testing, System Testing, Performance Testing, Integration Testing etc.
- III. The MSI shall perform the testing of the solution based on the test plan approved by ASCL
- IV. The MSI shall document the results and shall fix the bugs/ errors found during the testing
- V. It is the ultimate responsibility of MSI to ensure that the end product delivered meets all the requirements (including functional and technical requirements) specified in the RFP
- VI. The basic responsibility of testing the solution lies with the MSI

Deployment of ASCL Smart Solution Application

- I. The MSI shall deploy the Smart Solutions required for successful implementation of ASCL Smart City Implementation
- II. Data Migration/ Transition
- III. The MSI shall perform data migration/ transition activities (if any)
- IV. The data migration to be performed by the MSI shall be preceded by an appropriate data migration methodology, prepared by MSI and submitted to ASCL
- V. Any corrections, identified by ASCL in the data migration by Master System Integrator, shall be addressed by MSI at no additional cost to the ASCL

User Acceptance Testing

- I. The User Acceptance Testing of the software shall also be facilitated by the Master System Integrator. The detailed requirement has been specified in the RFP. Acceptance Testing shall involve:
 - Test Case development
 - Functional testing
 - Business case testing
 - MSI shall be required to bring its own testing tools for testing

Comprehensive Training

- I. MSI shall be required to provide training to all the ASCL staff or relevant stakeholders, to enable them to effectively operate and perform the relevant services using the solutions enabled by ASCL
- II. The training content shall be relevant to the target trainees depending upon the role played by them i.e. processing hands, technical/ administration personnel, supervisors/ managers, and senior officers etc.
- III. The MSI shall also be responsible for re-training the selected employees whenever major changes are made in the ASCL Smart Solutions
- IV. The Training shall be conducted in full synchronization with the overall Project Implementation plan
- V. MSI shall prepare a detailed training plan, including the method/ mode of training, training needs at various levels, the proposed curriculum, locations, material, duration of each training program and the entry and exit level criteria, and get it approved by ASCL before starting on the actual training
- VI. The language for training shall be both English and Punjabi

Ownership and Licenses

- I. The MSI shall provide licenses (perpetual) for application and all system software without constraints
 - II. All licenses shall be provided with lifetime validity and free updates/ upgrades/ patches during warranty and AMC period
 - III. The ownership of application and all system software designed, developed, procured, delivered, configured, and implemented for the Project shall lie with the ASCL
 - IV. All licenses would be in the name of "Amritsar Smart City Limited"
- b. Establishment of Test (Staging) & Development Environment
- I. It is proposed that the Test (staging) & Development environment architecture should be similar to that of production environment
 - II. All the components of the Test (staging) & Development environment application should be deployed in the similar way as they are deployed in the production environment (taking care of aspects such as clustering, integration etc.) This would streamline the process of testing before deployment on the production environment
- c. Requirement for Adherence to Standards
- I. The envisaged ASCL Smart Solution needs to be designed based on a prescribed set of Standards (as illustrated in Table below). These Standards would apply to all the aspects of the envisaged system including (but not limited) Design, Development, Procurement, Delivery, Configuration, Implementation, Testing, Data Migration, Commissioning, Operations & Maintenance and it is essential that the same are achieved and fully-adhered to during application maintenance period.
 - II. The application must be designed following open standards, to the extent feasible and in line with overall system requirements set out in this RFP, to provide for good interoperability with multiple platforms and avoid any technology or technology provider lock-in.
- d. Compliance with Industry Standards
- I. In addition to above, the proposed solution shall be based on and compliant with industry standards (their latest versions as on date) wherever applicable. There are many standards that are indicated throughout this RFP as well as summarized below. The list below is just for reference and is not to be treated as exhaustive.

Table 3-1- Industry Standards

S. No.	Component/ Application/ System	Prescribed Standard
1.	Workflow Design	WFMC/ BPM Standard
2.	Portal Development	W3C Specification
3.	Information Access/ Transfer Protocols	Simple Object Access Protocol, REST, HTTP/ HTTPS
4.	Interoperability	Web Services, Open Standard
5.	Document Encryption	PKCS specification
6.	Information Security	ISO 27001 certified system
7.	Operational Integrity & Security Maintenance	ISO 27002 certified system
8.	Operations	ISO 9001 certified
9.	IT Infrastructure Maintenance	ITIL/ EITM specification
10.	Service Maintenance	ISO 20000 specifications or latest
11.	Project Documentation	IEEE/ ISO specifications for documentation

3.14 Application Maintenance

- I. The MSI shall address all the errors/ bugs/ gaps in the functionality offered by solution (vis-à-vis the FRS or SRS or SDD signed off for Project) at no additional cost during the maintenance period
- II. MSI shall provide Bug Management Tool for tracking the status and closure of the bugs
- III. For performing of any functional changes to system that are deviating from the signed-off FRS or SRS or SDD, a separate Change Control Note (CCN) shall be prepared by MSI and the changes in the software shall be implemented accordingly. The period for implementation of change shall be mutually decided between the MSI and ASCL.
- IV. Modifications in the delivered ASCL Smart Solutions shall not be considered as Change request, only new requirement shall be considered as change request
- V. It is clarified that changes in Application, hardware and other IT Infrastructure required as a result of any legislative, administrative, policy changes by ASCL and workflow shall not constitute change of 'Scope of Work'
- VI. In case there is a change request in the Scope of Work, the MSI shall prepare the "CNS (change note on Scope of Work)" and get it approved by the department for the additional cost, effort and implementation time
- VII. The decision of ASCL on change being a CCN or CNS would be final & binding on Master System Integrator

3.15 Application Change & Version Control

- I. All planned changes to the ASCL Smart Solutions shall be coordinated within established Change Control processes to ensure that:
 - Appropriate communication on change required has taken place

- Proper approvals have been received
 - Schedules have been adjusted to minimize impact on the production environment
- II. The MSI shall define the Software Change Management & Version control process and obtain approval for the same from ASCL. For any changes to the ASCL Smart Solutions, MSI shall prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/ additional features added to the system etc. MSI is required to obtain approval from ASCL for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations & maintenance support.

3.16 Problem Identification and Resolution

- I. Identification and resolution of application problems (e.g. system malfunctions, performance problems and data corruption etc.) shall be part of Master System Integrator's responsibility
- II. The MSI shall also be responsible to rectify the defects pointed out by ASCL and carry out the enhancements suggested by them, as a result of the field assessments carried out by the ASCL, during the maintenance period. This shall be at no additional cost to the ASCL, in so far as the enhancements related to Scope of Work falling within the purview of the defined Scope of Work for Master System Integrator.
- III. Resolution of incidents/ problem logs created by the users of the ASCL Solutions

3.17 Provision, deployment and supervision of manpower for Operations & Maintenance of ASCL Smart Solutions

- I. The MSI shall be responsible for sourcing of the personnel and the management of all matters relating to such personnel, to carry out the responsibilities assigned to the MSI under the Contract. In particular, these shall include:
- Recruitment of the personnel possessing the qualifications prescribed in the RFP;
 - Training of the personnel;
 - Payment of salaries and benefits to the personnel;
 - Meeting all statutory obligations/ payments arising out of engaging the personnel;
 - Meeting all the liabilities arising out of the acts of the personnel
- II. During the course of the Contract, if it becomes necessary to replace any of the resource (due to non-performance or any other reason whatsoever), the MSI shall forthwith with due approval from ASCL, provide as a replacement a person of equivalent or better qualifications and experience than the resource being replaced/ or proposed in the bid

The team proposed by the MSI shall be on the rolls of the MSI(s) at the time of submission of the proposal. For any change of the resource or any resource being proposed for operations, the MSI should have to submit the CV of the resource, at least 2 weeks in advance for ASCL to decide on the replacement.

3.18 Training and Capacity Building

- I. MSI shall prepare and submit detailed User manuals to ASCL for review and approval.
- II. User Manuals shall be prepared in English, Hindi and Punjabi

- III. MSI shall impart operational and technical training to internal users on the infrastructure that is being used, its physical properties, usages and mechanism
- IV. MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Bi-Annual) to reflect the latest changes to the solutions implemented and new developments

3.19 Helpdesk

- I. MSI shall ensure helpdesk facility shall have following:
 - a. Call logging mechanism through Phone
 - b. Call logging mechanism through e-mail
 - c. Call logging mechanism through portal
- II. Helpdesk shall provide its services on all working days 24 X 7.
- III. All complaints/ grievances made by any mode shall be recorded and the records maintained for reference for a period of at least 3 months from the date of resolution of the problem
- IV. The MSI shall provide the following helpdesk performance monitoring reports:
 - a. Calls per week, month or another period
 - b. Numeric and graphical representation of call volume
 - c. Calls tracked by type
 - d. Number of dropped calls

3.20 Acceptance Testing

- I. Acceptance team/committee shall be constituted by the ASCL
- II. Detailed acceptance test procedures and test plans shall be submitted to ASCL for vetting before the start of commissioning of equipment.
 - a. Acceptance test plan describing the detailed schedule of primary and sub tasks shall be submitted to ASCL.
 - b. Acceptance test procedures as per the industry standards shall be submitted to ASCL.
 - c. Acceptance tests shall be carried out as per the accepted procedures and report shall be submitted for ASCL approval
- III. The primary goal of Acceptance Testing, Audit is to ensure that the solution meets Requirements, Standards, and Specifications as set out in the RFP and as needed to achieve the desired Output, Outcomes and Service Levels. The basic approach for this shall be ensuring that the following are associated with clear and quantifiable metrics for accountability:
 - a. Functional requirements
 - b. Availability of services in the defined locations
 - c. Performance
 - d. Security
 - e. Manageability
 - f. SLA Reporting System
 - g. Project Documentation
- IV. Complete testing of the solution shall be performed by MSI which includes but not limited to preparation of test script and running of test scripts. MSI shall get approved the same from ASCL.

- V. As part of Acceptance testing & audit, ASCL at any time may review all aspects of project development and implementation of ASCL Smart Solution including the processes relating to the design of solution and sub-systems, coding, testing, business process description, documentation, version control, change management, security, and performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the RFP
- VI. ASCL Smart Solution developed by the MSI shall be tested from security & controls perspective. Such testing shall also include the Application, IT Infrastructure and Network deployed for the ASCL Smart Solution. Following are the broad activities to be performed as part of Security Testing. The security testing shall subject the ASCL Smart Solution for the following activities:
 - a. Review of Server and Application security mechanisms
 - b. Assessment of authentication mechanism provided in the application/ components/ modules
 - c. Assessment of data encryption mechanisms implemented for the solution
 - d. Assessment of data access privileges, retention periods and archival mechanisms
 - e. Server and Application security features incorporated etc.
- VII. Performance is another key requirement for the ASCL Smart Solution and the MSI shall perform the Performance Testing of the deployed Solution against key parameters defined in SLA described in this RFP and/ or Contract between ASCL and Master System Integrator. Such parameters include request response time, work-flow processing time, concurrent sessions supported by the system. The performance review also includes verification of scalability provisioned in the application for catering to the requirements of volume growth in future.
- VIII. The application should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. ASCL shall perform various tests including server, security, DC failover tests to verify the availability of the services in case of component/ location failures.
- IX. MSI shall verify the manageability of the ASCL Smart Solution and its supporting sub-systems deployed using any enterprise management system proposed by the Master System Integrator. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc. shall be tested out.
- X. MSI shall develop/ procure/ customize and implement tools required to monitor the performance indicators listed under SLA prescribed in the RFP and calculations of scores accordingly
- XI. The MSI shall verify the Accuracy and Completeness of the information captured by the SLA monitoring system implemented shall certify the same
- XII. The MSI shall provide complete access to ASCL of the SLA tool(s).
- XIII. Upon completion of the testing, User Acceptance Testing shall be completed for a defined period
- XIV. Based on the testing, necessary recommendations of the committee shall be implemented before the commencement of the User Acceptance Testing period
- XV. Multiple User Acceptance Testing shall be required if ASCL to provide proof of operations and compliance to SLA's and performance criteria
- XVI. Detailed acceptance reports be submitted to ASCL office

- XVII. Necessary test and measurement equipment's/special tools for installation, testing and commissioning of the new components, for the purpose of initiating the operations & maintenance phase of new hardware should be made available by the MSI. Necessary calibration shall done and the certification of the same should be made available if requested by ASCL
- XVIII. ASCL team shall verify the component level details during the testing and shall sign the installation report after successful completion of the post installation testing activities. Defects / shortcomings brought out in this testing shall be attended as per the contract within the permitted time schedule

3.21 Go Live of the project

On successful acceptance of the User Acceptance Testing and based on test reports, the effective go-live date shall be decided by ASCL. The effective Go-live date shall be considered as the warranty date for all the equipment and devices.

3.22 Vendor Management

The vendor management activities shall include but not limited to:

- I. Coordination with all the project stakeholders (such as PMIDC, Project committees ASCL, MCA, User Departments, Vendors, if any) to ensure that all ICCC project related activities are carried out in a timely manner.
- II. Coordination with vendors and OEMs to ensure that time and equipment dependencies are optimally managed
- III. Coordinate and follow-up with all the relevant vendors of the State User Department to ensure that the user problems and issues are resolved in accordance with the SLAs agreed upon with them.
- IV. Ensure that unresolved issues are escalated to respective user departments.
- V. Maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.

4 Implementation Plan, Payment Schedule and Deliverables

Table 4-1 Implementation Plan, Payment Schedule and Deliverables

S. No.	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
1.	Project Award and Contract Signing between ASCL and successful Bidder	Project Start Date =T0		-
2.	Performance Bank Guarantee (PBG)		Performance Bank Guarantee (PBG) for the Project Term	-
3.	Team Deployment for the following: <ul style="list-style-type: none"> • Project Planning • Resource Scheduling • Development, Implementation & Maintenance approach 	T0 + 0.5	<ul style="list-style-type: none"> • Final Project Plan • Project Inception Report 	-
4.	Submission and approval of Site-survey Report (All tracks)	T0 + 2	<ul style="list-style-type: none"> • Solution Design Document • Final Survey Reports 	5 % of the CAPEX against Bank Guarantee of equivalent amount to be submitted along with the invoice for this milestone (shall be released within 15 days of the acceptance of the Solution Design Document and Final Survey Reports by the Technical Committee)
5.	Completion of Site preparation, Civil Works, HVAC Systems, Furniture and Electrical Work of Data Centre and ICC	T0 + 4	<ul style="list-style-type: none"> • Completion Reports • Inspection Reports approved by ASCL 	5 % of the CAPEX

S. No.	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
6.	Supply of all equipment/ components (Hardware) including System Software Licenses at the Data Centre and ICCC and all field equipment/ components (Hardware)	T0 + 7	<ul style="list-style-type: none"> • Delivery Challan with date & stamp on delivery proof • Copy/Original excise duty gate-pass • Inspection report from an authentic third party • Warranty certificate issued by respective OEMs for each hardware back to back in the name of "ASCL" • License in case of system software • Country of origin certificate 	15 % of the CAPEX
7.	Installation, Testing, Configuration and Operationalization of all	T0 + 10	<ul style="list-style-type: none"> • Device-wise configuration report stating IP schema • Installation, Testing and Commissioning Report • Complete set of Technical, Operations & Maintenance Manual • Configuration Change Report • Software Installation Guide and Checklist • Insurance certificate from the Insurance Company 	25 % of the CAPEX
8.	User Acceptance Testing, Training and Go-Live of all smart components	T0 + 12	<ul style="list-style-type: none"> • UAT Report • Training and Capacity Building • Defect Resolution Report • Commissioning Report • User Acceptance Testing and Go-Live of all Smart Solutions 	26 % of the CAPEX

S. No.	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
9.	Post Go-Live Support	48 months after effective Go-Live of Smart Solutions	<ul style="list-style-type: none"> SLA Adherence Report on a Monthly/Quarterly basis 	CAPEX amortized over 4 years: 24% (16 quarterly payments of 1.50% after in equated instalments after deductions of SLA penalties) AND OPEX amortized for 4 years payable quarterly at the end of each quarter in equated instalments after deductions of SLA penalties

- Additionally, all payments to be made by ASCL to the Bidder shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied/applicable (including GST as applicable). Any increase in rates of all applicable direct or indirect taxes (Central or State or local), rates, duties, charges and levies (Central or State or local), excluding GST shall be to the account of the Bidder. Any increase or decrease in the applicable tax shall be to the account of ASCL, for the services provided in this Contract. The invoices thus raised by the Bidder with Punjab GST Number.
- Any miscalculation of taxes by the Bidder shall be borne by the respective Bidder only, Purchaser shall not be liable for any miscalculation of taxes quoted by the Bidder in their Bid
- The Bidder shall also bear all personal/income taxes levied or imposed on its personnel on account of payment received under this Contract. Bidder shall further bear all income/corporate taxes, levied or imposed on account of payments received by it from ASCL for the work done under this Contract.
- CAPEX & OPEX ratio shall be reasonable and realistic, a bid shall not be considered for Final Evaluation if the total CAPEX value happens to be more than 50% of the overall bid value

5 Annexure I: Functional Requirements Specifications

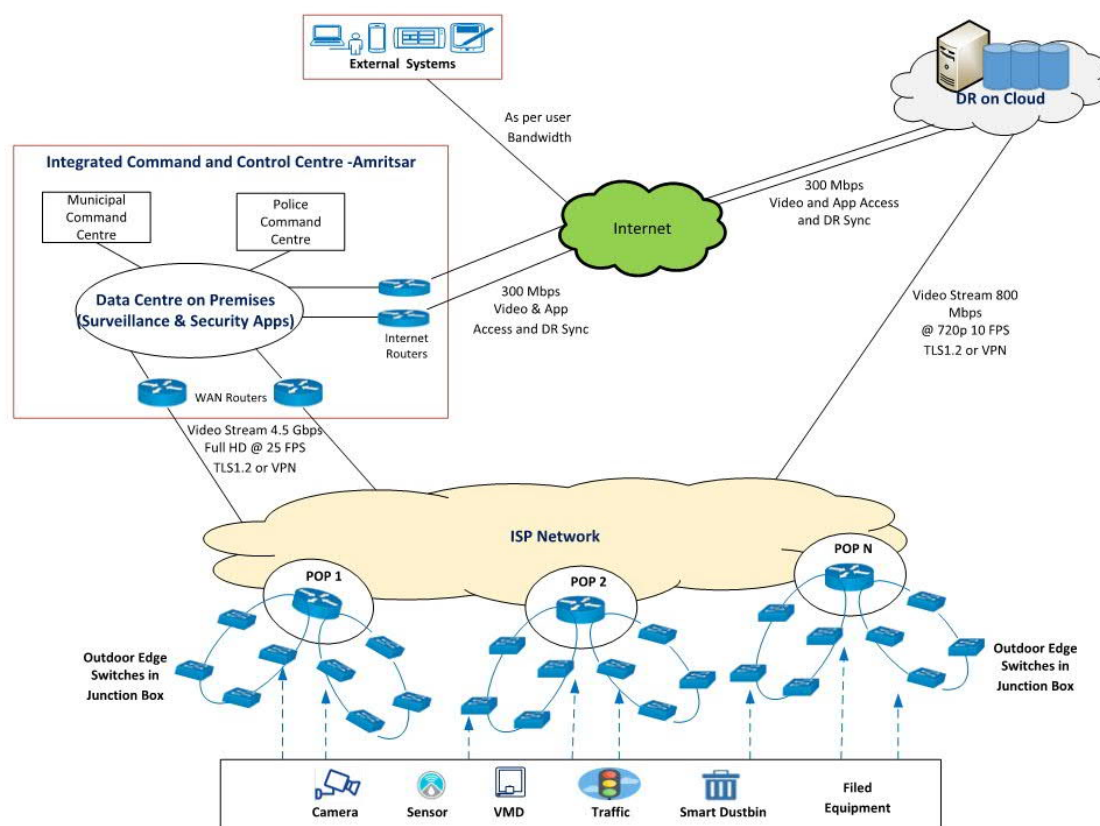
5.1 Field Infrastructure Functional Requirements

- I. Field switches shall be industrial grade robust & ruggedized switches that can work in outdoor environment.
- II. ISP shall connect all the junction boxes as per required bandwidth (MSI shall ensure the proposed bandwidth from each junction point is as per solution requirements)
- III. Central Authentication, Authorization and network device management server shall be placed in HA with required number of licenses.
- IV. Multiple Fixed Box/PTZ cameras and other field devices shall terminate on industrial grade Ethernet switch within Junction Box place in proximity to the end-points.
- V. Street layer devices like Variable Messaging Sign boards/PA systems/Emergency Call Boxes and other Smart City solution field devices will connect to nearest available industrial grade Ethernet switch within Junction Box
- VI. Sizing the Junction Box and provisioning of power is responsibility of MSI as per functional and technical requirements of this RFP
- VII. Total industrial grade Ethernet switches or other equipment in the junction box considered may vary depending on feasibility/nos. of devices and any extra industrial grade Ethernet switch or other equipment if required will responsibility of MSI as per as per functional and technical requirements of this RFP

5.2 Communication Network

- I. There shall be redundant network connectivity at Junction Box level. Typically, junction boxes shall be part of ring network as per MSI solution. The junction box shall continue to work at full capacity even if one side of the link is down.
- II. The redundant network links provided at Junction boxes shall be scalable to carry bandwidth up to 1Gbps each for future scalability. Actual bandwidth provisioned shall be as per solution design.
- III. City WAN network shall be aggregated into ISP links that shall be connected at Core routers at DC on Premise in high-availability mode and MSI should include required number & type of Ports in the core router to terminate the WAN ISP links with some spare ports for future use.
- IV. City WAN Network shall be aggregated into ISP links that shall connect to DR and DC in cloud. The MSI shall implement capability to route video and other traffic to DR when primary DC is not available. MSI shall provision this feature only when primary DC is not available and not send any duplicate streams to DR to optimize network usage.
- V. The core & Internet router interfaces shall be sized as per the termination links provided by ISP and shall meet all functional and technical requirements as mentioned in this RFP.
- VI. Network is taken on lease as a service, therefore all kinds of maintenance work or upgrades on the network shall be taken care by MSI at his own expense without any charge to ASCL.
- VII. The design and construction of network cabling used shall be inherently rugged and robust under all conditions of installation, operations, storage and transport.
- VIII. The network cabling shall be able to work in all field level environmental conditions and should be protected against corrosion or damage from rodents and other pests.
- IX. The MSI may choose to provide any type of last mile connectivity i.e. wired/wireless to meet the RFP requirements.

5.2.1 Logical Network Diagram



S. No	Link	Purpose	Estimated Bandwidth *
1.	Field devices to ISP network	Create aggregation link to transfer filed devices traffic to Data Centre	-
2.	ISP network to Data Centre on Premises	To transfer Full HD @ 25 FPS Video Stream data from ISP Network to local Data Centre	4.5 Gbps
3.	Field devices to Internet	To transfer IoT Data from Air Quality and Water Quality Analyser etc.to Internet	-
4.	Field to DR on Cloud	To transfer Video Stream 720P @ 10 FPS data from field equipment to Disaster Recovery on Cloud	800 Mbps
5.	DC on Premises to Internet	To sync Video and Application data from DC on premises to DR on Cloud.	300 Mbps
6.	Internet to DR on Cloud	To sync Video and Application data from DC on premises to DR on Cloud.	300 Mbps

*Note: - This is an estimated bandwidth MSI shall procure bandwidth as per their solution design and to meet requirements of ASCL as per the RFP.




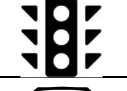








5.3 City Surveillance






5.3.1 Objectives of strengthening Security Surveillance

Objectives of strengthening Security Surveillance systems within Amritsar City are as follows:

- Instil confidence and create a sense of security among the people
- Reduce vandalism and efficiently protect citizens and property
- Identify and locate offender/s and criminals in the city
- Detect stolen/blacklisted vehicle movement in the city
- Optimize resource allocation for patrols, emergency response and other general duties
- Improve situational awareness and intelligence through utilization of digital imaging and video analytics
- Easy centralization of video surveillance operations and integration with other systems

Types of locations that may be considered for Security Surveillance system are presented below:

S. No.	Location Name	Type of location
1.	 Existing Cameras	All Existing IP Camera Location
2.	 Crime Hotspots	Major junction where Crime incident usually took place
3.	 Procession/Gathering Hotspots	Prominent locations where mostly crowd gathering events take place
4.	 Traffic Congestion Points	All Traffic Signals Railway station - inner and outer area with all entry & exit points
5.	 City Entry/Exit Points	All the entry and exit point of Amritsar
6.	 Railway Stations Entry/Exit Points	Railway station - inner and outer area with all entry & exit points
7.	 Bus Stations Entry/Exit Points	The entry and exit point of all the Bus Stations
8.	 Airport Entry / Exit Points	Entry and exit gate of Amritsar Airport road
9.	 Tourist Hotspots Entry/Exit Points	All the tourist departments
10.	 Main Markets Entry/Exit Points / Prime view	All exit and entry point of main market and prime locations
11.	 Schools	School entry and exit gate
12.	 Government Colleges (Entry/Exit Points)	Government College entry and exit gate

S. No.	Location Name		Type of location
13.		Government Hospitals	All areas around prominent hospitals in the City Prominent commercial area locations and complexes
14.		Traffic Junctions	All major traffic junctions of the city
15.		Parking Lots	IP Camera for Parking lots
16.		Administrative Building	In front of administrative building
17.		Government Infrastructure Assets	All Government infrastructure assets.

5.3.2 Surveillance System Sub-Components

- I. Surveillance system deployed by MSI shall have IP Cameras that generates real-time video streams, which are monitored, analysed and stored at ICCC for maintaining law and order in the city
- II. The MSI shall deploy Junction boxes at all identified locations to aggregate IP camera feeds and transmit them to ICCC over backhaul network leased from existing ISP's in the city
- III. The MSI shall supply Video Management and Recording application servers at the ICCC to administer the cameras remotely, real-time viewing of the cameras and recording the live video streams for a period of 30 Days for law and order function
- IV. The MSI shall provide both edge and server-side video analytics that can be applied to the video streams and alerts can be generated from it to escalate incidents in real-time for quick response
- V. The MSI shall also implement Facial Recognition System (FRS) on video streams to help the agencies deter criminal offences and safeguard public at airport, railway stations, bus stations, crime hotspots and city entry & exits
- VI. The MSI shall also implement Automatic Number Plate Recognition (ANPR) system on around 72 video streams to help the agencies identify and locate blacklisted vehicles at airport, railway stations, bus stations and city entry & exits
- VII. The MSI shall also implement Emergency Call Box with panic button at around 10 locations to help the citizens to reach the ICCC and facilitate reporting of emergency incidents to police from these locations in the city
- VIII. The MSI shall also implement an IP network based Public Address (PA) system at around 25 locations to help the police to control law and order and traffic from ICCC at these locations in the city. These locations shall also have PTZ and other cameras to support remote viewing and check adherence to instructions transmitted over PA system

S. No.	Servers	Description
1.	Video Management Server(s)	Video Management System Servers shall maintain coherent operations between all servers and workstations. It shall host Control Centre, where the system is administered, and System database. It shall monitor one or more Recorder servers on separate dedicated

S. No.	Servers	Description
		computers, storage devices, IP-compatible devices, and one or more workstation. All network communication shall also be is performed via the Video Management servers.
2.	Video Recording Server(s)	The Video Recorder Server shall be a dedicated server that shall store and processes video with the help of Video Management System
3.	Video Analytics Server (s)	Video Analytics Software shall be installed in the Video Analytics Server, to analyse live video in real-time to detect, identify, and track location, objects and people of interest. It shall automatically issue alerts to the appropriate personnel and initiate appropriate follow-up action according to predefined rules. This software shall also manage event detectors; each event detector shall monitor a single video feed for security events. The video feeds shall be connected over the network to the Video Analytics Server. Sensors on the Video Analytics Server shall perform all event detection functions. Analytics shall also include ANPR and Face Recognition systems at the ICCC.
4.	Web Server(s) and Thick Clients	Both Web Servers and thick client's interfaces shall be available to launch the client application remotely on web browsers or directly as an application installed on end viewing system.
5.	Gateway Server (s) (If required)	A Media Gateway server shall be used to establish remote connections to review and transcode the video. Standalone Media Gateway servers can also be installed on separate machines. Standalone servers shall be recommended for such large systems that shall transfer video data to remote clients.

5.3.3 General Functional Requirements

- I. All cameras supplied shall be for outdoor 24 X 7 operation with day and night operation with 4-year defect and damage replacement warranty
- II. All cameras shall be installed with
 - a. Pole erection as per standards to provide safety for mounted equipment
 - b. Electrical and Network wiring in conduits protected from environment, pests or other elements
 - c. Earth protection for poles and equipment
 - d. Environment protection rating as per standards for all equipment as per outdoor conditions in Amritsar
 - e. Mounting of all equipment shall meet weight and wind shear protection guidelines
 - f. Bird and pest protection measures for complete installation
 - g. External/Internal IR illuminators with minimum range of 100 meters
 - h. Tamper protection measures
 - i. Surge protection measures
 - j. Theft protection measures

- III. All cameras shall support H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG technology to reduce bandwidth and storage requirements of the system.
- IV. All field cameras shall be accessible over network from Data Centre (On Premise) and Disaster Recovery Centre in Cloud.
- V. All video feeds shall be either directly encrypted or carried through encrypted tunnel using VPN or HTTPS (TLS 1.2) with FIPS 140-2 Approved Security Functions with end to end encryption technology from cameras to video recording servers.
- VI. The cameras shall support only secure PKI certificate based authentication mechanism for both ONVIF and web based administrative access for the cameras. The certificate authority shall be secured using best in class technology in case of self-signed certificates.
- VII. All mounting, field of view and focal length adjustment for cameras shall be done in discussion with police department based on local surveillance requirements
- VIII. All cameras shall support minimum 2 streams with configurable resolution, framerate and compression that can be directed to any IP/URL address. It shall be possible to configure these streams for connectivity to ICCD Data Centre, Disaster Recovery Site (at a later date) and local police stations/LPU's etc. The deployed network shall have the capability to extend the feeds to Police Stations/Police HQs (if required).
- IX. Amritsar Police may review requirements for video resolution, FPS and may change these numbers to suit certain specific requirements at any given point.
- X. The system shall allow SMS and EMAIL alerts to be sent to any concerned person for escalation of a situation under a Standard Operating Procedure (SOP).
- XI. Housing of box camera and glass shall be certified by camera OEM or from the same camera OEM for optimal performance of the camera.
- XII. The MSI shall leverage GPU based processing for video analytics wherever possible to reduce the video analytics hardware server requirements and processing time.

5.3.4 Video Management & Recording System

S. No.	Minimum Requirement Description	Compliance (Yes / No)
1.	The proposed surveillance system shall support and integrate with the existing surveillance camera network in the city.	
2.	Video Management System (VMS) shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information for analysis.	
3.	The surveillance system shall be built on the open standards and should support ONVIF cameras and encoders.	
4.	The VMS shall be able to manage, display and record multiple video streams from a single IP camera or encoder	
5.	The surveillance system viewing system should be in thick client for local viewing and thin client through http browser for remote viewing. Both thin and thick client shall provide the capability of viewing single or multiple live and archive cameras.	
6.	VMS should allow managing initial client logon, system configurations, remote administration of recording servers, devices, security, rules, alerts and logging.	

S. No.	Minimum Requirement Description	Compliance (Yes / No)
7.	To ensure security and ease of Firewall deployment, only one Server should be allowed to be exposed to Internet for delivering services to all the remote clients sitting on the Internet. The remote clients should access only that server to access the system for all the functionality.	
8.	VMS application should provide mobile applications for Android & Apple devices. The application should allow viewing of live or archive videos and alerts.	
9.	All camera recordings shall have camera ID, location or area of recording and shall be programmable by the system administrator with user ID and password.	
10.	The VMS should allow creation of customised recording profile with all key camera parameters like resolution, frame rate, compression ratio, video streaming format etc. The operator should be able to select multiple available camera and apply profile to these cameras. It should be possible to assign the recording profile to an individual camera or a group of cameras or all cameras.	
11.	The VMS should allow selection of stream for recording.	
12.	The VMS should allow selection of single or group or all cameras for edge recording and sync recorded video with central server automatically after any network failure.	
13.	The VMS should allow the user to mark certain period of video recording as "critical data". Such critical data should be retained by the system irrespective of the camera recording storage configuration. There should be a possibility to move "Critical Data"	
14.	VMS should store all configuration data of Servers, Analytics Application Settings, Camera Recording Schedules, User Login Credentials, and Archived Video Files etc. in a relational database.	
15.	VMS should allow the users to download multiple segments of the video from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments should be downloaded in a single folder.	
16.	It should be possible to encrypt the exported video with password protection. The system should keep a record of such exported videos as audit trail.	
17.	The system should ensure that once recorded, the video cannot be altered; ensuring the audit trail is intact for evidential purposes.	
18.	It should be possible to create recording schedules on the fly, and assign any schedule to any camera, any group of cameras or to all the cameras any time. The recording should be controlled on hourly basis. It should be possible to manage recording on per camera basis, each with different video settings (e.g. format, frame rate and resolution).	
19.	The VMS should have a feature to restrict an operator to a particular hardware workstation only and have access to only those video streams for which he has permissions.	
20.	The VMS desktop client should be able to configure the entire system without any interface / operations required to be performed at the server level.	

S. No.	Minimum Requirement Description	Compliance (Yes / No)
21.	The VMS should store available screen layouts for each login user. The stored screen layout should be available on any of the operator workstations once the user logs-in.	
22.	The VMS desktop client should allow configuration of Video Management Server, Video Recorder Servers, Storage and Video Analytics and cameras.	
23.	<p>The System should support Maps integration in future with below features;</p> <ol style="list-style-type: none"> a. Adding Image Layers to the location map. b. Define the location map for each location. c. Add cameras to the map images. d. Add image layers to the map. e. Add a Maps Server <p>System should support raster format images of jpeg/jpg and png file and Vector (shape files)</p>	
24.	The VMS should show event notification from the cameras on the map itself. The operator should be able to click on the event notification of a particular camera on the map and the VMS should open the event window on the operator screen.	
25.	It should be possible to create a group of relevant cameras for simultaneous viewing. So, in case of an alert in one camera, the VMS should open the event window of the camera and show live video from other cameras in the group in a synchronised manner. It should also be possible for the operator to view the archive video from all the open cameras simultaneously, in a time synchronised manner.	
26.	The system should have PTZ camera control options within the matrix view of all the cameras. The PTZ controls should only be visible for PTZ camera/s. The operator should be able to control the PTZ camera within the matrix view itself.	
27.	The system should retain the VMS client screen state (including Video Analytics alert window, message window, Video Matrix, etc.) in case of an accidental shut down of the machine and should offer the exact same screen to the operator upon logging back into the system.	
28.	The VMS should allow creation of events for any camera from the drop-down menu. Such an event, when stored, should be searchable based on the camera, time, and event type. It should be possible to write description about the event.	
29.	The VMS should allow sending the event alert to the designated person or a group of designated persons through SMS or Email.	
30.	VMS should allow transferring the event alert to an administrator or another user registered in the system.	
31.	The VMS should allow monitoring of archive video of the selected camera under categories such as events, motion or continuous recording. The VMS	

S. No.	Minimum Requirement Description	Compliance (Yes / No)
	should also show a report of cameras indicating recording status for the selected duration, critical video data and Incident Video data.	
32.	VMS should allow camera clustering based on Locations as well as Groups independently. Each operator should be able to monitor one or several clusters of camera. VMS should be able to prevent an operator from viewing/managing one or several clusters.	
33.	<p>VMS should allow management of following typical camera parameters:</p> <ol style="list-style-type: none"> a. Brightness, compression, contrast, include date and time, resolution, rotation b. Frame per second, bit rate control mode, maximum bit rate, bit rate control priority, target bit rate c. Camera's Name, Description, Hardware name/Part number, Storage and recording settings, maximum storage limits and database configuration. d. Archiving settings e. Pre-set positions in case of a PTZ camera. f. Hardware configurable events 	
34.	The VMS should show the total hard drive space used to store the camera's recorded data. The storage media could be the DAS or SAN / NAS storage.	
35.	The Client Viewer should provide a Graphical User Interface (GUI) for the convenient access of live and recorded video as well as camera properties and display quality.	
36.	It should be possible to drag and drop cameras from the camera directory to the display screen.	
37.	The Client Viewer should offer the capability of browsing recordings from cameras on the same panel where other cameras are displayed live. There should be provision to replay multiple such cameras from various timestamps, independent to one another.	
38.	The Client viewer should have the feature to synchronize replay of selected cameras/all cameras in the view panel.	
39.	The Client Viewer should allow digital zooming on live view as well as on replay view on Fixed as well as PTZ Cameras.	
40.	The Client Viewer should support the use of keyboard shortcuts for control of standard features.	
41.	The Client Viewer should have the capability to receive multicast streams if a pre-set number of clients are requesting the same live view camera. The Operator should have the option to configure the system to always receive unicast streams at the discretion of the system administrator. The system should have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video.	
42.	The operator should have the ability to use digital zoom where the zooming is performed in the image only on any number of cameras	

S. No.	Minimum Requirement Description	Compliance (Yes / No)
	simultaneously. This functionality should be the default for fixed cameras. The use of digital zoom should not affect recording or other users.	
43.	Matrix Switching: The Client viewer should allow switching amongst multiple selected bookmarked display layouts with pre-determined time duration for each matrix view.	
44.	Video Stitching - The VMS should provide the ability for real-time video calibration tools providing stitched video view of areas that are covered by multiple cameras as a single image. The video stitching software module should provide the ability to "stitch" / integrate up to eight (8) cameras in any direction, horizontal, vertical and overlay to provide a single overlaid view of the selected cameras. It should also be possible to record such stitched view as one single video file for later retrieval.	
45.	Client viewer should allow the same camera to be viewed on multiple display tiles; one may be digitally zoomed, or on high resolution stream.	
46.	The Client Viewer should display Alerts defined as bookmarked events	
47.	The Client Viewer should allow an area of interest in an image to be searched for motion by time. Search parameters should include sensitivity and interval. A grid feature should allow only specific regions of interest to be searched.	
48.	The VMS should have capability to summarize activities in any given segment of video on demand, so that activities that happened during one hour of time can be viewed in e.g. less than 10 minutes without missing any activity.	
49.	It should be possible to navigate across multiple camera views simultaneously in a systematic way. By a simple copy-paste operation, it should be able to synchronize replays for any two or more cameras. On spot investigation of activities in the scene, with orchestrated use of Sitemap, Message Window and Virtual Matrix, should provide users with easy to use investigation tools.	
50.	VA should be able to follow movements of people, vehicles and other objects across multiple cameras in the archived video systematically and quickly, in a time synchronized fashion	

5.3.5 Video Analytics System

Video Analytics Software is a very important tool for Police to analyse events of interest which can be pre-defined based on the requirement. Also, the triggers generated can be sent to ICCG for immediate response and action on ground. The analytics software can bring significant benefit in analysing both live video feeds and recorded footages to review the incidences and look for suspicious activity.

The table below provides indicative break-up of camera locations with type of analytics and camera count at these locations

S. No.	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
1.	All Locations Fixed Cameras + PTZ + ANPR	<ul style="list-style-type: none"> • Video Recording • Camera Blocked • Camera Dusty • Camera Focus • Camera FOV Change • Privacy Protection 	21	35	78	778	130	72
2.	All Locations PTZ Cameras	<ul style="list-style-type: none"> • Automatic object/person recognition and tracking with PTZ cameras • Alarm object tracking from fix camera to PTZ camera • Alarm object tracking from PTZ camera to PTZ camera • Object tracking underneath the camera 	0	0	0	0	130	0
3.	Crime Hotspots	<ul style="list-style-type: none"> • Face Recognition • ANPR • Un-attended object origin search • Person of Interest Origin Search 	0	35	0	89	0	15

S. No.	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
		<ul style="list-style-type: none"> Loitering 						
4.	Procession/Protest Hotspots	<ul style="list-style-type: none"> Crowd Detection in Area of interest Un-attended object origin search Person of Interest Origin Search 	0	0	0	56	0	0
5.	Traffic Congestion Stretch	<ul style="list-style-type: none"> Traffic Congestion Detection (by Avg. Speed) Wrong Direction Traffic Flow 	0	0	0	18	0	0
6.	City Entry/Exit Points	<ul style="list-style-type: none"> ANPR 	0	0	0	0	0	42
7.	Railway Stations Entry/Exit Points	<ul style="list-style-type: none"> Face recognition=4 ANPR Un-attended object origin search Person of Interest Origin Search 	6	0	0	0	0	4
8.	Bus Stations Entry/Exit Points	<ul style="list-style-type: none"> Face recognition ANPR Un-attended object origin search Person of Interest Origin Search 	10	0	0	8	0	6
9.	Airport Entry / Exit Points	<ul style="list-style-type: none"> Face recognition ANPR Un-attended object origin search 	4	0	0	4	0	4

S. No.	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
		Person of Interest Origin Search						
10.	Tourist Hotspots Entry/Exit Points	<ul style="list-style-type: none"> Un-attended object origin search Person of Interest Origin Search 	0	0	0	12	0	0
11.	Main Markets Entry/Exit Points / Prime view	<ul style="list-style-type: none"> Un-attended object origin search Person of Interest Origin Search 	0	0	0	23	0	0
12.	Schools	<ul style="list-style-type: none"> Un-attended object origin search Person of Interest Origin Search 	0	0	0	9	0	0
13.	Government Colleges (Entry/Exit Points)	<ul style="list-style-type: none"> Un-attended object origin search Person of Interest Origin Search 	0	0	0	9	0	0
14.	Government Hospitals	<ul style="list-style-type: none"> Un-attended object origin search Person of Interest Origin Search 	0	0	0	50	0	0
15.	Traffic Junctions	<ul style="list-style-type: none"> Congestion Detection Wrong way driving 	0	0	0	12	0	
16.	Parking Lots	<ul style="list-style-type: none"> ANPR 	1	0	0	0	0	4
17.	Administrative Building	<ul style="list-style-type: none"> Motion Detection Indoor/Outdoor Trip Wire 	0	0	0	10	0	0
Total Video Analytics Cameras			42	70	78	1078	260	147

5.3.5.1. Video Analytics Functional Requirements

S. No.	Category	Minimum Requirement Specifications
1.	General Requirements	Proposed intelligent video analytics software shall have the capability to provide various alarms & triggers and should notified if any incidence/violation happens. Various video analytics that shall be offered on identified cameras are: <ul style="list-style-type: none"> • Person of Interest Origin Search • Unattended Object detection • Object tracking underneath the camera • Traffic Congestion Detection (by Avg. Speed) • Wrong Direction Traffic Flow/ Congestion Detection • Wrong way driving • Indoor/ Outdoor Trip Wire
2.	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
3.	General Requirements	The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.
4.	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
5.	General Requirements	The system shall allow the configuration of applicable rules and manage them.
6.	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size.
7.	General Requirements	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event
8.	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene
9.	General Requirements	The system shall enable detecting rules in the defined areas (zones/ lines)
10.	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.
11.	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately
12.	General Requirements	The system shall allow classification of different objects like animals, vehicles and people
13.	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.

S. No.	Category	Minimum Requirement Specifications
14.	General Requirements	Provide secured feeds with encryption, watermarking for data authenticity
15.	General Requirements	Trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.
16.	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system
17.	General Requirements	VAS should allow to add, edit, delete or disable and enable Policies.
18.	Features	The city-wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1:
19.	Security Features	Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA), Unattended object, Object Classification, Tripwire / Intrusion, Loitering, etc.
20.	Traffic / Parking Features	Vehicle Wrong Way Detection, Illegal Parking Detection, Congestion Detection, Vehicle Counting, Speeding Detection, Parking Management etc.
21.	Enhanced Monitoring Features	Video Stitching with Object Tracking, Video Stabilization, Video Smoke Detection, Video Fire Detection etc.
22.	Crowd Management	Crowd Control, Counter-Flow Detection, People Counting, Line Control, People Tracking etc.
23.	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)
24.	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification,
25.	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.
26.	General Requirements	The system shall allow classification of different objects like animals, vehicles, people etc.
27.	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events such as motion Detection etc. as picked up by Camera without the need for human intervention
28.	General Requirements	Provide secured feeds with encryption, watermarking for data authenticity

S. No.	Category	Minimum Requirement Specifications
29.	General Requirements	Trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.
30.	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system
31.	General Requirements	Allow to add, edit, delete or disable and enable Policies
32.	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence
33.	General Requirements	The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.
34.	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
35.	General Requirements	The system shall allow the configuration of applicable rules and manage them.
36.	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size
37.	General Requirements	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event
38.	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene
39.	General Requirements	The system shall enable detecting rules in the defined areas (zones/lines)
40.	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.
41.	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately
42.	Features	<p>The city-wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1:</p> <ol style="list-style-type: none"> Parking Violation Wrong Direction People loitering Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA) Unattended Object

S. No.	Category	Minimum Requirement Specifications
		<ul style="list-style-type: none"> f. Crowd detection g. Traffic flow/Congestion h. Traffic Volume estimation and statistical counts i. People tracking
43.	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)
44.	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification
45.	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.
46.	Edge Analytics	<ul style="list-style-type: none"> • Auto Tracker: To detect and track movement in the field of view. • Adaptive Motion Detection: To detect and track object that enter a scene and then triggers an alarm when the object enters a user-defined zone. • Abandoned Object: To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows. • Camera Sabotage: Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap. • Directional Motion: Generates an alarm in a high traffic area when a person or object moves in a specified direction. • Object Removal: To triggers an alarm if the object is removed from a user-defined zone. • Stopped Vehicle: To detect vehicles stopped near a sensitive area longer than the user-defined time allows. • Intrusion Detection – Detect intrusion

5.3.5.2. Built-in-Edge Analytics for the Cameras

The surveillance system shall support following Built-in-Edge Analytics for the Cameras:

- I. Auto Tracker: To detect and track movement in the field of view.
- II. Adaptive Motion Detection: To detect and track object that enter a scene and then triggers an alarm when the object enters a user-defined zone.
- III. Abandoned Object: To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows.
- IV. Camera Sabotage: Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap.
- V. Directional Motion: Generates an alarm in a high traffic area when a person or object moves

in a specified direction.

- VI. Object Removal: To triggers an alarm if the object is removed from a user-defined zone.
- VII. Stopped Vehicle: To detect vehicles stopped near a sensitive area longer than the user-defined time allows.
- VIII. Intrusion Detection – Detect intrusion

5.3.6 Body Camera

S. No.	Minimum Requirement Description
1.	Cameras shall have the ability to be mountable on several locations including, but not limited to: <ul style="list-style-type: none"> •Shoulder •Helmet •Collar •Sunglasses and Headband •Epaulet •Vehicle •Other
2.	Captured images from software/video shall export in the following formats: <ul style="list-style-type: none"> • JPEG • TIFF • BMP • PNG
3.	The total number of wire or cable connections for the worn devices
4.	Shall have camera data storage that is secure and Non-removable is preferred.
5.	If camera uses removable storage: Removable camera storage shall prevent copying, deleting, tampering, modifying video using any third-party tools. Requires VMS or proprietary access to memory card –no third-party tool access allowed.
6.	Shall have image stabilization capability
7.	Shall have capability to stream video wirelessly from camera to Command Centre VMS/Video Recording Server over 4G/LTE
8.	Streaming live view Capability
9.	Shall support MP3 audio format
10.	Administrator shall be able to configure video settings or have selectable bit rate (multiple settings to allow optimization of file size and upload speed)
11.	Shall be able to export video format and be compatible with the following: <ul style="list-style-type: none"> • MP4 • AVI • WMV • WAV • MOV • H.264/H.265 • MPEG • DIVX
12.	Shall have capability to control the volume for audio and visual play back

5.4 Public Address (PA) System

S. No.	Minimum Requirement Specifications
1.	The PAS can be used by ASCL, Police and other stake-holders of the project to disseminate information to road users/public.
2.	The objective of the voice based sub-system is to disseminate the information to the citizens particularly during emergencies for the messages to reach quickly.
3.	The system should have the capability of designing the messages based on the situation or context for broadcasting across PAS.
4.	The software and solution of PAS shall comply with all functional and business requirement as specified in this RFP.
5.	The PA system shall provide provision for emergency announcements to be made on per-location, selection of locations, or a system wide basis.
6.	The PA system shall have provision for announcements to be made from two central locations.
7.	The Integrated Traffic Management system shall provide for the ability to produce and play-out either pre-recorded messages or make live announcements through PA software.
8.	The PA system shall be integrated with the Integrated Traffic Management & Emergency Response Management System for making automated, system generated, or manual announcements as per the SOPs.
9.	The system should have ability to integrate with CCTV systems, other main/sub systems at ICCC for configuring and broadcasting the messages.
10.	The system should have ability to configure the messages with the static or dynamic text from various applications/systems to form a complete message as and when required.
11.	The system should recognize and broadcast messages based on some of the analytics such as sound alerts, system alerts, incident alerts and various other alerts.
12.	The System should be able to integrate other networks PA system of third party application systems where the alerts are generated to broadcast messages.
13.	There shall be an operator at central control room to operate the PAS application on PAS console.
14.	The system should be able to generate various statistics, reports & MIS from time to time
15.	The system shall be designed and installed so that it automatically minimizes community sound pollution
16.	The requirements of local noise level standards & by-laws shall be respected by this system.
17.	The system should have the ability to schedule category wise system messages or overall messages in advance for a period of time to selective or all PAS locations.
18.	The PAS message quality shall be such that it is clearly audible from its location to a distance of more than 100m without any distortion and loss in quality of the sound during the prevailing situation in street.
19.	Ability to integrate with CCTV systems, VMD and other main/sub systems at Command Centre for configuring and broadcasting the messages to the road users.
20.	Ability to configure the messages with the static or dynamic text from various applications/systems to form a complete message as and when required.

S. No.	Minimum Requirement Specifications
21.	Ability to categorize the messages as per the business need and able to configure as per category.
22.	The PAS should provide the status indicators on the system and as well at various command centre
23.	The PA system shall have an operations monitoring dashboard, located at the control centre
24.	On this dashboard there shall be a schematic layout of the PA system showing all the connected nodes on the GUI.
25.	The various nodes when connected & disconnected shall be represented in different colour schema on the GUI of the Control Centre operator.
26.	If any particular node is disconnected from the control room, the same shall raise an alarm to the ICCC operator GUI & appropriate action shall be taken to rectify the same.
27.	The monitoring dashboard shall allow the ICCC operator to click on any node & view the details of "Operator" logged in, time duration since logged in, summary of operations If ICCC operator or any other user form ICCC disable/enable/operate any active device remotely, the same shall be captured in ICCC activity report with all details including but not limited to date, time, device, action performed etc.
28.	The monitoring dashboard shall show the status (connected/disconnected, faulty/working) of all logical devices (PA system) connected to a particular node when clicking on a node from the monitoring dashboard GUI.
29.	In case of any fault in the devices connected to a node, or connectivity failure with a node, a pop-up message shall appear on the monitoring dashboard workstation. The operator has to acknowledge the pop-up message & report the type of fault to the maintenance team & shall record the details to the assigned team/individual into the system.
30.	Fault assignment to the maintenance team shall be managed and controlled by the system software only. Once a fault is assigned by the ICCC operator or authorized user to the maintenance team, the same shall be displayed in the maintenance module and once fault is closed/resolved by the maintenance team it shall be updated automatically (in case of active devices) or else updated manually in the software application/maintenance module.
31.	The access to monitoring dashboard shall be specific to the privilege of the user which can be defined in the system & shall be specific to a group/part of node locations.

5.5 Emergency Call Box (ECB) System

S. No	Parameters	Minimum Functional Requirement
1.	Functional Specification	<ul style="list-style-type: none"> The emergency call box (with panic button) will enable citizens to establish a two-way audio (microphone and speaker) & camera (video camera) communication link with Police (or / and with Authority's Disaster Management Cell or Command and Control Centre or Dial 112 or other location as per requirement of Police department) through a press of a button.

S. No	Parameters	Minimum Functional Requirement
		<ul style="list-style-type: none"> Emergency Call Box shall be strategically located at locations accessible to public, suitably sized and identified/clearly labelled for "Emergency". The unit shall preferably have a single button which when pressed, shall connect to Authority.
2.	General Requirement	The ECB locations shall be determined by Police Department (mostly near junction boxes in the city to avoid any additional investments).
3.	General Requirement	These are to be placed only select locations such as Police/Traffic islands or pedestals or within the vicinity of constant Police supervision or IP camera field of view to avoid misuse and vandalism of the call box.

5.6 Variable Message Display (VMD)

S. No	Functional Specification	Minimum Requirement
1.	System Requirements	<ul style="list-style-type: none"> The system should be capable to display warnings, traffic advice, route guidance, air quality, traffic congestion, live journey time, alternate routes to destination, weather updates, emergency messages and any other dynamic messages automatically from the cloud. For live journey time and congestion levels, VMS solution shall be capable to draw the information on its own and take the data feed from the cloud (e.g. google cloud etc.) and work in an automated fashion depending on GPS location of a VMS. The real-time information can also be pushed manually from ICCC as well as system should capable to take the data from the cloud for display on the board. MSI shall build all the above capabilities in their offering. The system should also be capable to display warnings, traffic advice, route Guidance and emergency messages to motorist. Emergency messages can also be distributed to specific/all VMS board via secure mobile and tablet communication. The VMS should display text (multi lingual – Hindi, Punjabi & English) and Graphic messages using Light Emitting Diode (LED) arrays. The System should support Display characters in true type fonts and adjustable based on the Operating system requirement. The VMS workstation at the ICCC should communicate with the VMS controller through the network and cloud hosted application. It should send out command data to the variable message sign controller and to confirm normal operation of

S. No	Functional Specification	Minimum Requirement
		<p>the signboard. In return, the VMS workstation should receive status data from the VMS controller.</p> <ul style="list-style-type: none"> • VMS 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 online software hosted in Public Cloud. • It shall be capable of setting an individual VMS or group of VMS'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 VMS or a group of VMSs at a pre-set date and time. • 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. VMS shall use 128-bit encryption to ensure downloads/transfer of files • Display should be CE, FCC, CB certified • VMS shall also be able to work individually providing real-time information in an automated manner even in the case of connectivity loss between central server and LED Board • The digital media player/thin client on the LED display shall have minimum 4 GB, RAM and 16 GB flash memory with at least 1.5 Ghz processor for playing rich content and for integration with sensors • VMS shall have an option to view latest content screenshot of every display on the centrally hosted VMS application in Public Cloud. The system shall maintain the history of messages archived for future reference and analysis
2.	Variable Message Sign board application	<ul style="list-style-type: none"> • Central Control Software allows controlling multiple VMS (unlimited perpetual license) 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 • 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

S. No	Functional Specification	Minimum Requirement
		<ul style="list-style-type: none"> • 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 Traffic Monitoring Centre 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. • 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 • Facility to export reports to excel and PDF formats

S. No	Functional Specification	Minimum Requirement
3.	Remote Monitoring	<ul style="list-style-type: none"> • All VMS shall be connected/ configured to ICCG 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 reason of failure up to the level of failed Individual LED

5.7 Air Quality Monitoring System

a. Air Quality Monitoring Stations

- I. Environmental sensor station shall monitor following additional parameters and include the following integrated sensors inside one station:
 - SO₂
 - NO₂
 - CO
 - CO₂
 - O₃
 - PM₁₀
 - PM_{2.5}
 - Noise pollution
 - Temperature
 - Humidity
- II. It shall be an integrated station which shall monitor overall ambient air, light and noise quality among other parameters as detailed in point above
- III. Air Quality monitoring station shall be ruggedized enough to be deployed in open air areas such as Industrial area, Markets, important bus stands and parks.
- IV. Air Quality Monitoring Systems shall be placed at approx. 7 locations in Amritsar as per Annexure - V.

b. Central Environment System

- I. The Central Air Quality Monitoring software (AQMS) would be hosted in Public Cloud with unlimited devices perpetual license.
- II. All Air Quality Monitoring stations shall be integrated with centralized monitoring software.
- III. Software shall display real-time and historical data in chart and table views for dashboard view of the Client
- IV. Software shall display trends of environmental parameters based on user specific time periods
- V. It shall be possible to configure and calibrate the sensors through the software from a remote location
- VI. Alarms shall be generated for events where the environmental parameters breach the safe or normal levels

- VII. Amritsar Smart City Limited/Pollution Control Board should be able to configure or change the erroneous environmental parameters.
 - VIII. These Air Quality Monitoring stations shall sense the prevailing environment conditions and send the data to the AQMS, where real-time data shall be analysed, presented on dashboard with alerts.
 - IX. The AQMS shall also be integrated with the state and central pollution control board website and database via API integration to share data with them on regular intervals.
- c. Digital Display Unit
- I. The collated environmental information shall be relayed instantaneously to local Variable Messaging Sign Boards (VMS) mounted on poles alongside the Air Quality Monitoring Stations which let citizens know the prevalent environmental conditions.
 - II. A Digital display software system shall be provided in Public Cloud for message preparation, monitoring and control of the VMS. The VMS shall communicate with ICCCL using an IP based network.
 - III. The Digital display software application should accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client.
 - IV. Software should be GUI based, and capable to handle multiple VMS. User should be able to select desired location on the Map and the live status of that specific Air Quality Monitoring Station and associated VMS.

5.8 Online Water Quality Analyser

- I. The micro-station for waste water shall be supplied for online monitoring of water quality parameters in waste water. The required components: Spectro-probes and controller shall be the factory assembled with all required flow cells, mounting fittings and pipes in to a compact panel.
- II. The micro station shall include a micro-controller based remote terminal unit for data acquisition, data display and station control. The process connection shall be through PVC pipes with probes installed within flow cell. The micro station shall include compressor for pressurized automated cleaning
- III. It shall provide the pressurized air for automatic cleaning of the probes. The device shall be designed for online monitoring of below mentioned quality parameters at Tung dhab and City Outfall drain
- IV. T Micro station data including water quality parameters and maintenance data shall be transmitted wirelessly for remote monitoring.
- V. Following table describes the details of probe ranges, accuracy and the type of parameters to be measured at the Tung dhab and City Outfall drain

The major prerequisites of efficient online analysers are as follows:

- I. The Quality Monitoring Controllers / Analysers shall produce accurate output with high precision and repeatability
- II. MSI shall install robust and rugged instrument/analyser, for optimal operation under extreme waste water conditions, while maintaining its calibrated status.
- III. The Quality analyser / Controllers supplied, shall have inbuilt features for automatic water matrix change adaption

- IV. The OWQM station controller shall have remote system access from central server for provisioning and log file access.
- V. The OWQM station controller shall have provision for data transmission from each station without intermediate PC or plant server directly over 3G/4G/LTE network.
- VI. It shall have provision to send system alarm to central server in case any changes made in configuration or calibration.
- VII. Should have provision to record all operation information in log file.
- VIII. For each parameter there shall be provision for independent analysis, validation, calibration & data transmission.
- IX. Must have provision of a system memory (non-volatile) to record data for at-least one year of continuous operation.
- X. Should have provision of Plant level data viewing and retrieval with selection of Ethernet, wireless, Modbus & USB.
- XI. The correlation/interpretation factor for estimating COD and BOD using UV-Visible Absorption Technique shall be regularly authenticated/ validated and details provided
- XII. Record of calibration and validation should be available on real-time basis on central server from each location/parameter
- XIII. Record of online diagnostic features including sensor status should be available in database for user friendly maintenance
- XIV. Expandable program to calculate parameter load daily, weekly or monthly basis for future evaluation with flow rate signal input
- XV. Must have low operation and maintenance requirements with low chemical consumption and recurring cost of consumables and spares

The MSI shall ensure that the measurement shall be performed in-situ, without sampling or sample pre-treatment, thus preventing errors due to sampling, sample transport and storage etc. The measurement cycle shall be between 20 and 60 seconds, making possible a high measuring frequency and detection of rapid changes in water quality.

5.9 Data Centre on Premise

- I. Amritsar Smart City Data centre architecture shall categorized in three zones with the help of Spine and leaf architecture as per below mentioned.
 - a. External zone shall consist of termination points for Internet & City WAN Network ISP links and a DMZ zone that shall be create for accessing the public servers from internet.
 - b. Internal zone shall consist of a MZ & DMZ zone.
 - a. The Internal DMZ zone shall consist of all Security, Collaboration, Monitoring, Application performance and management devices shall be placed which shall be accessed from the NOC and Control and Command Rooms.
 - b. The MZ zone shall consist of the Compute & Storage hardware, Smart city application software, Surveillance & unified storage and other systems that will have restricted access.
- II. Proposed solution shall meet the minimum following
 - a. Internet Links shall be terminated at internet routers in high-availability mode

- b. City WAN network shall be aggregated into ISP links that shall be connected at Core router in high-availability mode and MSI should include required number & type of Ports in the core router to terminate the WAN ISP links with some spare ports for future use.
- c. Internet firewall shall be proposed with Next Generation Firewall including IPS & Anti-Malware Protection and Anti-APT functionality to protect the data centre network from internet born threats and shall be placed at perimeter level.
- d. Core firewall shall be placed at between core network components and internal data centre as a 2nd layer of defence of the data centre network.
- e. Network Behaviour Analysis flow collector & sensors shall be placed at perimeter level for continuous real-time monitoring & pervasive view of all network traffic.
- f. Data centre switching architecture shall be based on spine-leaf architecture wherein all the devices should connect to leaf switches and Spine switch should connect to leaf switches over high speed connectivity
- g. All the L4-L7 devices (Anti-APT, Server Load Balancer, WAF, Policy Server, NBA, EMS etc.) shall connect to Leaf switches over multiple 1/10G Ethernet links.
- h. The compute infrastructure shall also connect to leaf switches over multiple of 10G connectivity's
- i. Surveillance and Unified Storage shall connect to leaf switches or compute infra through SAN switch as per solution.
- j. Solution should provide efficient service chaining for providing advanced security with Virtual IPS, Firewall for Applications.

5.10 General Requirements of Public Cloud Infrastructure

The MSI shall be responsible to ensure that CSP's selected shall meet all the below functional requirements and include them as part of their solution design and proposal

5.10.1 General Requirements

- I. ASCL shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
- II. The respective Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
- III. CSPs shall provide interoperability support with regards to available APIs, data portability etc. for the Government Department to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
- IV. Bidder should ensure security, compliance, visibility, control of applications running in public cloud.
- V. MSI should ensure portability of applications from on premise to CSP cloud, back to on premise cloud by use of standard formats to avoid cloud silos and to avoid application refactoring.
- VI. MSI should ensure security and compliance of applications and data by maintaining consistent network and security policies across on premise and CSP cloud. The network and security

policies should follow Virtual Machines as it moves within and across CSP and on-premise Data Centre.

- VII. MSI should provide solution for automated failover and recovery of application VMs in proper sequence to CSP data Centre and should provide solution to perform DR drill for full and selected applications every quarter without impacting production applications running in primary environment.

5.10.2 Availability and SLAs

- I. The Primary and Disaster Recovery cloud services shall be hosted by CSP's as per MEITY approved guidelines.
- II. Minimum 99.5% up time measured monthly for availability of the virtual machines at the respective Data Centre site.
- III. The bidder shall have IP v6 support or roadmap for its cloud services.
- IV. The cloud provider should have the ability to automatically make multiple redundant copies of user data in primary as well as disaster recovery Data Centre.
- V. The integrated minimum SLA of 99.9 availability shall be provided for database and other service components.

5.10.3 Cloud: Functional Requirements

- I. The proposed application cloud environment should provide flexibility to scale the environment vertically and horizontally:
 - a. Vertically: Upscale/downscale the solution to higher configuration Virtual Machines (i.e. VMs with different combinations of CPU and Memory)
 - b. Horizontally: Add more Virtual Machines of the same configuration to a load balanced pool.

It should be possible to scale the solution vertically/horizontally at any time, without prior notification to the cloud provider. It should be possible to automate this process of scaling up and down automatically.

- II. The cloud data centre must have assured protection with security built at multiple levels and 24x7 monitoring by provisioning physical security, biometric identification and close circuit monitoring.
- III. It should be possible at any time to move the Cloud Virtual Machines to ASCL's Datacentre/s running industry leading Hyper Visors. The mechanism and technical requirements for achieving this should be well documented.
- IV. The CSP should provide all variants of cloud service – Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)

5.10.4 Service Management and provisioning

- I. Provide the ability to provision virtual machines, storage and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
- II. Cloud Management interface should have the ability to unilaterally provision and de-provision the specific IaaS services contemplated by the project via Web Portal, Command Line Interface

and Web Services Application Programming Interface (“API”). All the communication for these purposes should be secured at transport level using SSL / TLS and or SSH.

- III. The CSP shall manage the underlying hardware infrastructure and virtualization layer following the appropriate patch management and technology refresh cycles.
- IV. The CSP shall provide mechanisms to enable data isolation and privacy in its environment.

5.10.5 User / administrative management

- I. The Proposer shall support multiple users with a management portal.
- II. The Proposer shall provide Billing / Invoice tracking through a web portal aggregated by user application and service at mutually agreed intervals.
- III. Service Provider should provide multi-factor authentication for accessing the cloud infrastructure and application
- IV. The CSP should provide Role Based Access Control to segregate users based on their roles and privileges.
- V. The CSP should provide the capability to log operations being conducted on the infrastructure.
- VI. The CSP should provide ability to set up alerts and monitoring for different parameters to track health and usage of the infrastructure.
- VII. Cloud provider should offer a service health dashboard that displays up-to-the-minute information on service availability across multiple regions with 365-day SLA history.
- VIII. Cloud provider should offer a support service to help provision resources by following best practices.
- IX. The CSP should provide monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.
- X. Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.
- XI. Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing

5.10.6 Integration

- I. The CSP shall provide an API for each of the required services that enables the development of complex automation solution for resource provisioning, configuration and de-provisioning.
- II. The APIs should be based on open interoperable standard such as REST.

- III. The CSP shall provide APIs to consume the services and complete documentation for all the APIs it offers.
- IV. CSP platform should support multiple operating systems, at a minimum Windows, Red Hat Linux and Ubuntu.
- V. The CSP shall support SDKs for this APIs for at least Microsoft .net and Java/JavaScript.
- VI. The CSP should provide API management features as a native capability; It should provide real-time analytics and enable trend identifications on the usage of the published API's; Should provide a single place to manage all APIs.
- VII. Each solution area should be modularized to auto scale independently and on-demand.

5.10.7 Network Services

- I. The CSP shall provide IP addressing that will support: DHCP, IP address and port assignment on external (public) interfaces, dedicated VPN connectivity and the ability to map Project DNS domains to CSP services addresses enabling services, sites and applications operating in the CSP infrastructure to be viewed as URLs.
- II. The service should provide a traffic management mechanism to implement both performance and availability-based load balancing for virtual Machine Instances.
- III. The CSP should provide virtual private network (VPN) connectivity from cloud environment in both Site-to-Site and Point-to-Site configurations.
- IV. The service provider should provide an option of extending an MPLS to cloud.
- V. The services provider's infrastructure should be protected against DDoS
- VI. The solution must provide virtual network isolation capabilities among the virtual machines must support the use of private VLANs
- VII. The cloud service provider shall have multiple Tier 1 ISPs providing Internet connectivity to their datacentre / network.
- VIII. The CSP should provide connectivity with options to leverage carrier provided MPLS and should be backed by SLA.
- IX. Direct peering with Telco service providers for speedy and efficient delivery of content to all users accessing the service from various devices on various network service providers is a must.
- X. CSP shall have the capability to provide adequate bandwidth between Primary Data Centre and Disaster Recovery Centre for data replication purpose.
- XI. The CSP should support network level redundancy through MPLS lines from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc. These two network service providers should not share same back end infrastructure.
- XII. The CSP should be able to offer adequate link connectivity to cloud through MPLS as per MSI solution design
- XIII. The CSP should have adequate internet capacity at each Cloud data Centre as per MSI solution design.

5.10.8 Security, Privacy and Compliance Requirement

- I. The infrastructure elements including server, storage (including backup storage) and network of the Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from other tenants.
- II. The entire N/W Path for each of the hosted government applications shall be separate (logical separation & isolation) from the other clients (including other government departments).
- III. CSP should enable encryption of data both in rest and transit.
- IV. CSP should provide flexibility to choose various firewall and router solutions from the industry leading vendors.
- V. The cloud service offering shall support Network and security with virtual firewall and virtual load balancer integration for auto-scale functions.
- VI. Must have Separate VLAN provision with dedicated virtual firewall between the VLANs and for each client.
- VII. Conduct regular independent third-party assessments of the CSP's security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome. CSP should make these reports available to ASCL via secure portal.
- VIII. Allow penetration testing to be done by scheduling it in advance.
- IX. The CSP should provide a multi-tenant, Identity management (User Authentication & Authorization) and Directory service as a cloud service (as a native platform feature) backed by SLA. The Identity service should allow single sign-on (SSO).

5.10.9 Interoperability

A large variety of cloud services has led to proprietary architectures and technologies being used by vendors, increasing the risk of vendor lock-in for customers. ASCL needs to avoid the problem of vendor lock-in, where they run the risk of being tied to a particular cloud service provider due to the difficulty and costs of switching to use equivalent cloud services from other providers. MSI shall ensure interoperability to avoid the incidents such as a cloud service provider shutting down operations or the discovery of significant security vulnerabilities in applications.

- a. The proposed solution must provide flexibility to move the application and its associated data from private cloud/on premise data centre to a public cloud, across two different public cloud providers and from Public Cloud to private cloud/on premise data centre. This movement can be required during exit management, capacity building purpose and to maintain data interoperability among various cloud service providers. This movement of data should be carried out over the network in an online fashion without requiring cumbersome and time-consuming backup and recovery procedures. To ensure security and reduce the bandwidth required for this purpose, the data movement must be encrypted and should provide deduplication and compression. Any software/hardware required to meet this requirement should be provided as part of the proposed solution.
- b. The proposed solution should allow flexibility to allow solution components to be hosted on a public or private cloud and its DR to be hosted on another public or private cloud. To ensure security and reduce the bandwidth required for this purpose, the data movement must be encrypted and should provide deduplication and compression. Any software/hardware required to meet this requirement should be provided as part of the proposed solution.

- c. The proposed solution should provide flexibility to backup applications and data from public/private cloud/on premise data centre to another public/private cloud/on premise data centre. To ensure security and reduce the bandwidth required for this purpose, the data movement must be encrypted and should provide deduplication and compression. Any software/hardware required to meet this requirement should be provided as part of the proposed solution.
- d. The applications leveraging the cloud infrastructure should use non-proprietary protocols and APIs so that applications can be migrated from a private cloud/on-premise data centre to a public cloud, across two different public cloud providers and from Public Cloud to Private Cloud/on-premise data centre without any need to carry any customization. Any software/hardware required to meet this requirement should be provided as part of the proposed solution.

5.11 Data Centre on Cloud

Functional Requirements provided under are indicative, MSI carefully examine the requirements and may propose technical specification / design as per their solution to meet the objective of RFP.

- I. Design Guidelines
 - a. The MSI shall propose Public Cloud services only from the MeitY approved and empanelled Cloud Service Provider (CSP's). The CSP should have cleared the STQC audit as mandated by MEITY as on date of submission of bids to be considered as valid. The vendors should be fully compliant with all guidelines issued by MeitY namely
 - o Guidelines for Government Departments for Adoption / Procurement of Cloud Services
 - o Guidelines for Government Departments on Service Level Agreement for Procuring Cloud Services
 - o Guidelines for Government Departments on Contractual Terms Related to Cloud Services
 - b. The CSP's regional nodes which are used for hosting the infrastructure including disaster recovery shall be within India.
 - c. The hosting environment shall be a Public Cloud which shall be connected to City Operation Centre via VPN once it is available. The SI shall be responsible to provision necessary VPN termination infrastructure (e.g., Virtual private gateway, NAT, VPN Software etc.) on Public Cloud side for such connectivity.
 - d. The MSI shall plan for pre-production environments for Development, Testing and Staging of any application change requirements, patches or upgrades and shall deploy them in production only upon approval from ASCL.

5.12 Disaster Recovery on Cloud

- I. There should be logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers on Private cloud.
- II. The cameras shall operate at lower settings i.e. 720P @ 10 FPS in case of DR scenario. This setting profile shall be applied by VMS on cloud on field cameras to reduce bitrate in DR scenario. ANPR cameras shall operate at 720p@ 25 FPS.
- III. All applications in scope shall be operational from DR site after DC is not available as per RTO/RPO guideline.

- IV. Viewing bandwidth shall be provisioned for minimum of 100 cameras streams at 720P and 10 FPS at one time in DR scenario. During the period of disaster, it shall be possible to view video feeds from multiple police viewing centres or personal computers.
- V. All the important video evidence shall be moved to unified storage on regular basis with help police personnel (ideally within 7 days). The complete application databases, tagged video evidence data and other important data and files on 125 TB unified storage shall be replicated in cloud on based on RPO/RTO guidelines. It shall be duty of MSI to delete data after requisite permissions from police department.
- VI. All applications except Video Analytics & Face Recognition shall be operational. ANPR shall be functional in DR scenario.
- VII. The camera stream to DR shall be activated only in DR Scenario to reduce bandwidth cost.
- VIII. It is expected that MSI shall make all necessary provision to ensure high availability at the Data Centre and after switching over to the DR; it gets back in to normal operations from the DC as soon as possible. However, the overall disaster Recovery Solution should be provisioned in such a manner that previous 7 days feeds are available and it should be able to run for 7 Days in case of Disaster.
- IX. One full-scale DR drill to be conducted during UAT & post go-live and additional DR Drills on quarterly yearly basis shall be conducted. Total DR period in a year shall be assumed to be 24 days a year for purpose of sizing including DR drills
- X. The system shall be hosted in the site identified by the MSI and as agreed by the ASCL for DR in a different seismic zone.
- XI. There should be sufficient capacity (compute, network and storage capacity offered) available for near real-time performance (as per the SLA requirement of the ASCL) during any unanticipated spikes in the user load.
- XII. DR site shall be located in India only.
- XIII. The design ensure redundancy at each level
- XIV. ASCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the ASCL's application. ASCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time
- XV. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.999%, SLA measured at the VM Level & SLA measured at the Storage Levels
- XVI. The following cloud software and services should active and be accessible via internet and MPLS:
 - a. Video Management and Recording Servers providing Live Video Feeds (max simultaneous during DR shall be 100)
 - b. ANPR Servers
 - c. Public Address System Software
 - d. Air Quality Monitoring Software Servers
 - e. Variable Message Display Software
 - f. Online Water Quality Management Software
 - g. Help Desk and Incident Management Software
- XVII. MSI shall provide complete SLA Management during DR Scenario for which he can leverage cloud monitoring tools of CSP to create SLA reports.
- XVIII. Required Support to be provided to the ASCL in migration of the VMs, data, content and any other assets to the new environment created by the ASCL or any Agency (on behalf of the

ASCL) on alternate cloud service provider's offerings to enable successful deployment and running of the ASCL's solution on the new infrastructure.

- Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
- For the files, perform weekly backups;
- For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
- 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.
- Retain database backups for thirty (30) days

Preparation of Disaster Recovery Operational Plan

The MSI should provide detailed operating procedures for each application during the following scenarios. These shall be mutually agreed upon with ASCL during the project kick off.

- I. Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary (DR) site.
- II. Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
- III. Operations from DR site: Ensuring secondary site is addressing the functionality as desired

Periodic Disaster Recovery Plan Update

The MSI shall be responsible for –

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

Configure proposed solution for usage

The MSI shall provide DR Management Solution to ASCL meeting following specifications:

S. No.	Minimum Requirement Description
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

S. No.	Minimum Requirement Description
5.	The proposed solution should facilitate out-of-the-box, 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
7.	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8.	The proposed solution must support all major platforms including Linux, Windows, Solaris, and Unix etc. with high availability options. It must support both physical and virtual platforms
9.	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10.	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11.	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned
12.	The proposed solution should be capable of understanding the application level interdependencies Automatically and the prioritization of application recovery tiers to ensure Application availability at DR during disaster situations
13.	Proposed solution should be able to monitor performance and utilization of the business services and their respective IT components like CPU/Memory/application services using the SNMP v3 to provide the root cause and impact of any disruption and its cascading effect.
14.	The proposed solution shall showcase the Business service availability and integration with IT in real-time hierarchy shown and the cascading impact of disruption on multiple business services along with financial impact
15.	The proposed solution should be able to auto build the workflow/runbook from the manual DR drill that we do. Vendors should be able to build/generate the Runbook in the real-time automatically while we perform the manual DR Drill
16.	The proposed solutions shall have workflows to recover all the layers of a business applications includes Application, OS, database, Network, Storage
17.	The proposed solution should have Ready-to-build solution templates and designers available out-of-the-box to recover Applications quickly and easily.
18.	The proposed solution shall be agent-less Discovery of Application Interdependency and Application Infrastructure.
19.	The proposed solution should be capable of building and deploying various connectors to monitor and orchestrate different technologies pertaining to Applications on the fly without involving any onsite development efforts

5.13 Integrated Command Control Centre

5.13.1 ICCC Platform Functional Requirements

- I. The Platform shall be a fully integrated portal-based solution that provides seamless incident–response management, collaboration and geo-spatial display.
- II. The Platform shall provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, the platform shall provide a Common Operating Picture (COP) of various events in real-time on a unified platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.
- III. The platform should have high processing power and adequate data storage with a high-performance information highway to provide process information in real-time and serving decision support system. The platform should also provide portability to meet changing city scenario. The MSI is required to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved.
- IV. The solution should be capable of seamless integration to various government and emergency services such as law enforcement, disaster and emergency services, utility services etc.
- V. The platform shall support adding more layers of solutions seamlessly with minimal effort which the municipality/development authority intends to develop in time to come (But not limited to mentioned solution only).
- VI. On the ICCC platform, the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on the Authorities policies and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation. The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users.
- VII. The inputs/feeds from the different components of Smart City Solutions shall be received at Integrated Command and Control centre video wall for monitoring, tracking and decision support purpose on real-time basis supported with GIS technology. Further, operators shall be working on their respective monitors for assessing the inputs and triggering actions at ground level.
- VIII. MSI needs to conduct a detailed assessment, design a comprehensive technical architecture, implement and operate the common Integrated Command & Control Centre Platform.
- IX. The proposed Integrated Command & Control Centre Platform shall be hosted at data centre and all field level smart cities use cases needs to be integrated with this platform. City level applications like ERP, E-governance, taxes and all other business application shall also be integrated with ICCC platform to read & analyse data from those application to visualize on ICCC dashboard.
- X. Proposed ICCC architecture should be combination key functionalities like Data Normalization, IoT Platform, API Manager/Gateway, Database and City operation centre software.
- XI. Data Aggregation & Normalization Layer must integrate City urban services as per current & future need of city and must deliver an architecture which shall be future scalable to accommodate more urban services & Applications.

- XII. Data from this aggregation & normalization layer shall be used for urban services/applications management & Control & customized Reporting's. Also, this layer should provide the data to various cities partners/application developers via API to develop citizen centric applications, portal and mobile applications etc.
- XIII. MSI needs to conduct a detailed assessment, design a comprehensive technical architecture, implement and operate the common Integrated Common Command & Control platform.
- XIV. All field level smart cities use cases needs to be integrated with this platform. City level applications like ERP, E-governance, taxes and all other business application (In future) shall also be integrated with platform to read & analyse data from those application to visualize on City level CCC (Command & control Centre) dashboard
- XV. Proposed Solution architecture should have combination of data normalization (IoT Platform) and City operation centre software functionalities covering Complex Event Processing, Rules Engine, Map and Video Based Visualization.
- XVI. Data Aggregation & Normalization Layer must integrate City urban services as per current need of city and must deliver an architecture which shall be future scalable to accommodate more urban services & Applications.
- XVII. Data from this aggregation & normalization layer shall be used for urban services/applications management & Control and customized reporting's.

5.13.2 Network Operation Centre (NOC) Functional Requirements

- I. NOC shall monitor all the infrastructure devices (Router, switches, firewall, advance security component, bandwidth, Application performance etc.) that are kept in core locations, aggregation layer along with key services that shall be provisioned in due course.
- II. NOC Shall help in monitoring the issues related to fibre, network, and infrastructure implemented, Applications and Platforms and provide help desk system for the same.
- III. Configurations and Change Management: Configuration shall be managed from core locations for all the devices/sensors on the network. For any change applicable, based on the type/severity/complexity of change, the change should be proposed with due justification and to be implemented upon approval from ASCL.
- IV. The proposed solution shall have redundancy built at each layer.
- V. The proposed solution shall be ready in all respect where it is envisaged by ASCL to make use of this infrastructure under different revenue models under its long-term vision.
- VI. The solution shall meet demands of bandwidth needs for all the procured and planned smart city solutions in near future (Applicable for Core component in Data centre)
- VII. The key functionalities of the NOC shall include
 - a. Incident Management based on resource workload, incident Category etc.
 - b. Tracking and reporting of all contractual SLAs in an automated way.
 - c. Updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
 - d. The NOC shall escalate issues in a hierarchical manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation.
- VIII. Primary responsibilities of NOC personnel shall include but not limited to:
 - a. Network Supervision and Monitoring: Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode

- b. Configuration Management: Ensure the proper configuration of network, systems and applications or the provision of reliable and high-quality end-user services
 - c. Change Management, Network Extension: Ensure efficient day-to-day management of short-term network changes and optimization, including their implementation. This activity shall be synchronized with the maintenance scheduled activities
 - d. Performance Management: Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
 - e. Service and Network Provisioning: Define all necessary actions to be performed when a request for a new service is issued, and control the actions performed at NOC level or field level until completion
 - f. Scheduled Activities Planning: Provide regular plans for all scheduled activities, including preventive maintenance. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities
 - g. IT and DB Management: Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
 - h. Security Management: Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
 - i. Quality Management: Define quality management policies, and ensure implementation and usage for competitive quality of service
 - j. Workforce Management: Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
 - k. Inventory Management: Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
 - l. Spare Parts Management: Manage spare part handling and logistics to minimize repair/swap turn-around times for defective items, & keep low CAPEX for spare parts and consumables
 - m. Asset Inventory Management: Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
 - n. Repair and Return: Receive and repair defective boards, return repaired or replacement boards.
- IX. The MSI shall ensure adherence to the following prerequisites:
- a. All the IT devices that are installed by the MSI shall be Simple Network Management Protocol ('SNMP') enabled and the MSI shall centrally and remotely monitor and manage the devices on a 24x7x365 basis. It should also be provisioned to bring Non-IT components on the common monitoring
 - b. MSI shall provide on-site comprehensive maintenance of the entire IT / Non-IT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance of respective project phase. The individual project phases will run independently.
 - c. MSI shall operate and maintain the Network infrastructure (Active / Passive / Physical) as per well-defined Standard Operating Procedures.
 - d. MSI to establish and implement leading practices of IT service Management like Information Technology Infrastructure Library (ITIL), International Organization for

- Standardization (ISO)/IEC 20000 standard that shall promote the adoption of an integrated approach to effectively deliver managed services to meet the requirements.
- e. MSI shall identify all assets and document the importance of these assets. The asset inventory shall include all the information necessary in order to recover from a disaster, including type of assets, format, location, backup information, license information etc.
 - f. MSI shall undertake scheduled and ad hoc maintenance (on need basis) and operations like configuration backup, patch management and upgrades
 - g. MSI shall establish basic tools for IT and Non-IT management to undertake health check monitoring, troubleshooting etc. for all Network operations
 - h. MSI shall establish access control mechanism and shift wise attendance management system
 - i. The MSI shall ensure that all resident engineers in the NOC are certified (of the OEMs of the network components) and are provided at Command and Control Centre for 24/7 operations.
- X. Typical Network Infrastructure Management Services shall include
- a. MSI shall ensure that the network is available 24x7x365 as per the prescribed SLAs
 - b. MSI shall provide services for management of network environment to maintain performance at optimum levels.
 - c. MSI shall be responsible for attending to and resolving network failures and snags
 - d. MSI shall support and maintain overall network infrastructure including but not limited to WAN/LAN passive components, routers, switches, Firewalls', IPS/IDS, Load Balancers etc.
 - e. MSI shall Configure and backup network devices including documentation of all configurations
 - f. MSI shall provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers
 - g. MSI shall create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users.
 - h. MSI shall provide a single-point-of-contact for requesting any service. The Network Administrator shall respond to the initial request from the user groups within the agreed service levels and service coverage hours.
 - i. MSI shall provide support as required to assist in hardware and software problem isolation and resolution in the LAN/WAN environment.
 - j. MSI shall perform LAN/WAN problem determination.
 - k. MSI shall communicate changes affecting the LAN/WAN environment.
 - l. MSI shall maintain LAN/WAN configuration data.
 - m. MSI shall be responsible for polling / collecting of network devices security logs from all the systems. All these logs shall be made available to the Enterprise Management System (EMS) solution
- XI. Security Administration and Management Services:
- Management of security environment of the entire network infrastructure to maintain performance at optimum levels.

- Address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, and vulnerability protection through implementation of proper patches and rules.
- Maintain an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, including, but not limited to, operating systems, security solutions, network solutions, etc.
- Ensure that patches / workarounds for identified vulnerabilities are patched / blocked immediately.
- Respond to security breaches or other security incidents and coordinate with respective OEM in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, firewalls, servers, desktops from viruses.
- Operating system hardening through appropriate configuration and patch updates on a regular basis.

XII. Physical & Environmental Security at locations

- Ensure that all network switches are secured and are enabled only when required by authorized employees.
- Perform reactive and preventive maintenance exercise
- Monitor the environmental controls for security of network equipment, cabling security and IT hardware management.
- Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001, BS 7799 and BS 15000 guidelines

5.13.3 Cyber Security Framework

The security events that are of significance in the ICCC network infrastructure and the protection mechanisms/ technologies against the same are indicated in the table below:

S. No.	Area of focus	Description	Devices/ Technologies
1.	Access Security	Protecting against unauthenticated devices from sending information to the Integrated Command & Control Centre (ICCC).	Authentication, Authorization and Accounting (AAA)
2.	Transport Security	Prevent any eavesdropping on the network by sniffing data on the network.	Access control and secure encrypted transport over network like Leased line/ SDWAN/MPLS networks
3.	ICCC Security	Preventing any illegitimate traffic from entering the ICCC from the access network. Preventing attacks on one component of the ICCC solution	Internet & Internal Firewall. Network Behavioural Analysis and Detection. Web security devices.

S. No.	Area of focus	Description	Devices/ Technologies
		<p>from impacting other solutions/ components.</p> <p>Preventing any unauthorized access into the ICCC from the Internet through emails, or web browsing.</p> <p>Baselining the normal traffic patterns in the smart city network infrastructure and detecting for any deviations from the baseline.</p> <p>Preventing against any malicious files that can transform after coming into the network (Advanced Persistent Threats).</p> <p>Preventing users and systems from within the ICCC to access any malicious sites even before they initiate the request.</p>	Anti-APT solutions on network perimeter like email and web gateways.
4.	Services Security	Ensuring that the smart city services are always available to the users/ citizens, and are not impacted by any DDoS attacks.	Application DDoS protection systems.
5.	Security Operations	<p>Ensuring that the security logs are analysed proactively, and the traffic and data patterns analysed for proactive threat hunting.</p> <p>Ensure that if a security incident occurs, it is detected, contained and mitigated in a fast and effective manner to prevent the spread of the infection.</p>	Managed Detection and Response Services coupled with threat intelligence services by MSI.

As per the minimum-security requirements below are the security capabilities which will be required as minimum within the IT infrastructure

5.13.3.1. Network Behaviour Analysis & Detection

Propose required solution for network behaviour anomaly detection, full packet capture and forensic requirements.

Network Behaviour analysis is an Integral part of today's cyber security solution as it provides entire visibility of network like who is doing what by capturing raw packets continuously on the network and therefore provides the capability to go back in time and investigate an indicator-of-compromise. Some of the Functional Features that shall provide visibility into network and detect threats proactively are as below:

I. Visibility & Identity Awareness

- a. NBA Solution shall provide the internal network visibility by capturing all packets that traverse the specific network segment and thus provide actionable insight required to quickly identify and troubleshoot a wide variety of network issues.
- II. Troubleshooting
 - a. NBA Solution shall also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. It will also provide root cause analysis capabilities, web session regeneration capabilities and perform full reconstruction of assets transferred, accessed and transmitted
- III. Forensics and Incident Response
 - a. By collecting, analysing and storing large amounts of raw packet data, NBA System provides a full trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.

5.13.3.2. Authentication, Authorization and Accounting (AAA)

- I. Solution shall provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; BYOD, and guest management services on a single platform. Shall allow admin to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy.
- II. AAA shall control the network with predefined policies, including pre-admission endpoint security policy checks and post-admission controls defining which users and devices can connect to the network, and what network segments can they access.
- III. Shall allow to authenticate and authorize users and endpoints via wired, wireless and VPN with consistent policy throughout the enterprise and support variety of authentication methods with Dual Stack / Layer mode.
- IV. The system needs to integrate with end-point Antimalware, anti-virus solution or any other solution for mitigation of non-zero-day attacks, and shall support Security compliance policy for antivirus, patch update, operating system version etc.
- V. The system shall have programmable external facing interfaces, providing OPEN APIs to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.
- VI. The system shall include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable integration with firewall, IPS, Router, Switch, Wireless Access Points, Active Directory, LDAP, MDM, SIEM solutions, ticketing systems etc. of major OEMs.

5.13.3.3. Internal and Internet Firewalls

The appliance based security platform shall be capable of application visibility, and control, VPN functionality in a single appliance. Also uses open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats. Supports multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).

- I. The firewall shall be a next generation appliance capable of providing firewall features, application visibility.
- II. Shall provide application detection for commonly used protocols like DNS, FTP, HTTP, SMTP, ESMTP, LDAP, MGCP, RTSP, SIP, SQLNET, TFTP, H.323, SNMP etc.
- III. Support for access-rules for both IPv4 & IPv6 objects simultaneously with detecting & blocking malware and sandboxing, as per the guidelines defined in the section Protection against

Advanced Malware and have a rich set of Northbound APIs for it to be integrated into a SIEM system.

5.13.3.4. Intrusion Prevention system

- I. The IPS shall accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, Do's, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection, malformed traffic etc.
- II. Shall detect and block all known, high risk exploits along with their underlying vulnerability and not just one exploit of that vulnerability.
- III. Shall support traffic inspection for IPv6, IPv4, and Tunnelled: 4in6, 6in4, 6to4 traffic.
- IV. Support for ingestion of threat intelligence feeds like IP reputation intelligence feeds, URL & DNS threat intelligence feeds and SNORT signatures.
- V. Shall have 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.

5.13.3.5. Web Security Solution

- I. Appliance Requirement and Functionality: Shall be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities shall be in a single appliance only. Option to run Advance Malware Protection engine utilizing sand boxing technology for file and file reputation analysis.
- II. Secure Remote Access: Critical feature of the solution as web security shall be deployed across an organization. Support Team shall be able to login to appliance using secure tunnelling methods such as SSH for troubleshooting purposes.
- III. Forward proxy mode - Single and Dual IP configuration: Forward proxy mode deployment solution to support single / Dual IP proxy configuration where one IP will be of local LAN and another IP will be of DMZ.
- IV. Support multiple deployment options: The solution shall allow to deploy the appliance in explicit proxy as well as transparent mode together.

5.13.3.6. Anti-APT

Advanced persistent threat (APT) is a network stealthy attack in which an unauthorized person gains access to a network or an endpoint and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. Solution should be a single unified solution that uncovers, prioritizes, and remediates advanced attacks. The product should use intelligence from endpoint, network, and email control points, as well as global threat intelligence, to stop threats that evade individual security products.

- Uncover, prioritize, and remediate advanced attacks across all endpoints while adding advanced Endpoint Detection and Response (EDR) capabilities.
- Uncover and prioritize advanced attacks coming into the network and detect suspicious activity happening within your organization.
- Cover advanced attacks entering your organization through email, by adding unique targeted attack identification

Advanced Threat Protection should provide a single console showing all suspicious events and attacks across the organization, allowing all data and intelligence about any attack, across endpoint, network, and email, to be shown in one place. Solution shall be capable of working in Inline Blocking mode without depending on other network components like a separate FW, IPS or Web Security Appliance.

5.13.3.7. Web Application Firewall

Overall solution shall have web application firewall (or WAF) functionality to filter, monitor, and block HTTP traffic to and from a web application. WAF shall be able to filter the content of specific web applications. By inspecting HTTP traffic, it shall prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

The proposed Web Application Security architecture should identify complex attack chains, and not just aggregate events based on attacks or sources.

The proposed Web Application Security architecture should provide advanced and proactive BOT detection mechanism based on smart combination of signature-based and heuristic analysis. It should also have ability to detect Bots which can execute JavaScript.

The proposed Web Application Security architecture should be able to encrypt the user credentials in real-time to protect the credentials especially password/Aadhar number or any other sensitive parameter as defined by department to protect from keyloggers and credential stealing malware residing in the end user's system browser.

The proposed Web Application Security architecture should prevent of theft as well as mitigation of attacks that uses stolen credentials.

5.13.4 Seating Capacity and IT/Non- IT Equipment

S. No.	Room Description	Expected Seating capacity	Mandatory or optional	Tentative Computer Equipment
1.	Reception	1 Person	Mandatory	Personal Computer with Visitor Management Logging- 1 No.
2.	Police Control Room	11 People – 9 Operator and 2 Supervisors for Police Functions	Mandatory	<ul style="list-style-type: none"> • Personal Computer with work stations - 18 Nos with 3 Monitor for each PC • Heavy Duty All in one Printer - 1 No. • Video Wall 4 X 2, 50" Cube – 1 No. • Video Wall 4 X 2, 50" Cube – 1 No. • IP Phones – 12 No.
	Municipal Control Room	11 People – 9 operators and 2 Supervisors for Municipal Functions	Mandatory	
3.	NOC Room	08 People	Mandatory	Work Stations or Laptop for 08 People as per requirement
4.	Data centre - Farm Area (4 Racks)	4 Racks with space for expansion to 8 racks	Mandatory	Including server and network racks

S. No.	Room Description	Expected Seating capacity	Mandatory or optional	Tentative Computer Equipment
5.	Telecommunications Room	1 telecom racks with space for expansion to 2 racks	Mandatory	Including server and network racks
6.	Conference Room/War Room	12 People with LAN connectivity	Mandatory	12 People Seating capacity with furniture. Size may be reduced if required in final design.
7.	Staging room	1 Rack and 1 Personnel computer	Mandatory	Rack -1 and PC -1
8.	Power Distribution Panel Room & Battery Room	Switching panels and electrical devices	Mandatory	-
9.	Building Management System Room with staff	04 People including supervisor.	Mandatory	Personnel Computer – 04 Nos. with BMS Systems
10.	PAC in the farm area	2 nos. or as per requirements	Mandatory	-
11.	DG with Fuel Tank	2 nos. or as per requirement	Mandatory	-
12.	Sub Station / Transformer	2 nos. or as per requirement	Mandatory	-
13.	Earth Pits	As per requirement	Mandatory	-

5.13.5 Non- IT – Data Centre Civil & Architectural work

S. No.	Component	Guidelines / Specifications/Scope
1.	General	<p>The scope for civil work in this RFP is to furnish the data Centre area in all aspects. The furnishing includes but not limited to the following:</p> <ul style="list-style-type: none"> • Cement Concrete Work • Cutting and chipping of existing floors • Trench works • Masonry works • Hardware and Metals • Glazing • Paint work • False Flooring • False Ceiling • Storage • Furniture & fixture • Partitioning

S. No.	Component	Guidelines / Specifications/Scope
		<ul style="list-style-type: none"> • Doors and Locking • Painting • Fire proofing all surfaces • Insulating
2.	Raised Flooring	<ul style="list-style-type: none"> • Providing & fixing steel cementitious raised access floor of FFH up to 450mm finished with antistatic high pressure laminate in size 600 X 600 mm X 35 mm with point load 450 kg and uniform distribution load (UDL) 1350 kg per sq. metre as per following specifications: Panel Type - M 1000, Under structure- Edge Support Rigid Grid, Wear resistance (g / cm²) - < 0.08, Bottom profile - Hemispherical shape, Pedestal -all steel construction & silver zinc plated, Exposed surface- Special weather coating on entire surface of the tiles. The same should also be provided with wire manager and tile lifter etc. • At least 1' 6" High from existing floor level using antistatic laminated tiles. • Supply & Fixing of 1.5 mm Antistatic Laminate skirting matching with floor tiles with 8mm thick MDF Board / Bison Board up to a height of 4". • Supplying and fixing vinyl flooring with homogeneous flexible vinyl flooring of approved shade 2.0 mm thick in roll forms and manufacturers specification over the existing floor. Before laying, the existing flooring should be made free from dust and undulations. The finished flooring should be free from air bubbles and thoroughly cleaned without undulations. • Providing and laying premium quality Granite white/ cream tiles of size 2'-0" X 2'-0", 8.5 mm thick set in cement mortar and pointing with approved tile joint filler compound of approved make of matching shade as per manufacturer's specification as directed. The work shall include the preparation of base surface, cleaning, and acid wash. • do - for skirting up to a height of 4" • Providing and fixing 9 mm thick floor insulation below the false flooring and joints should be finished properly as per manufacturer's specification
3.	False Ceiling	<ul style="list-style-type: none"> • Providing and fixing 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

S. No.	Component	Guidelines / Specifications/Scope
		<p>inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles and 25mm thick glass wool of 16kg.sq.m density wrapped on both sides with aluminium foil and placed over each tile etc.</p> <ul style="list-style-type: none"> • Providing and fixing 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. Area of electrical fixtures will be paid full fixed to G.I. supports to receive spotlights including cutting hole etc., complete. G.I. metal frame to be of 24-gauge folded strip of 50mm width to be used. GI vertical supports to be anchored to slab by means of anchor fasteners.
4.	Furniture and Fixture	<ul style="list-style-type: none"> • Workstation size of 2' depth made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. The desk top will be 25mm thick & edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per design, complete with approved quality drawer slides, hinges, locks etc. • 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"x1'9"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish • Cabin table of depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. • Providing, making & fixing 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.

S. No.	Component	Guidelines / Specifications/Scope
		<ul style="list-style-type: none"> • Providing, making & fixing 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. • Fire proof safe (300 Litres. or above) with one-hour fire rated.
5.	Partitions	<ul style="list-style-type: none"> • Providing and fixing in position 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 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating. • With glazing including the framework of 4" X 2" powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas). • Providing & fixing 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. • Providing & fixing Fire Rated Wire Glass minimum 6 mm thick for the partition wall between the Server Farm Area I of approx. 1585 sq. and Server Farm Area II of approx. 963 sq. complete with all the required accessories • Provide glass partitioning including privacy screen/blinds between the ICCC Room and War Room.
6.	Painting	<ul style="list-style-type: none"> • Providing and applying Fire retardant paint of approved make and shade to give an even shade over a primer coat as per manufacturers' recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer's recommendation for coverage of paint. • For all vertical Plain surface. • For fire line gyp-board ceiling.

S. No.	Component	Guidelines / Specifications/Scope
		<ul style="list-style-type: none"> • Providing and laying POP punning over cement plaster in perfect line and level with thickness of 10 - 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc. • Applying approved fire-retardant coating on all vertical surfaces, furniture etc. as per manufacturer's specification.
7.	Civil Work	<ul style="list-style-type: none"> • Providing and laying 115 mm thick brick work in cement mortar of 1:4 (1 cement: 4 sand) with bricks of approved quality chamber bricks of class designation 50. • Providing & making SS signage with text in etched & black painted to be located as directed (wall mounted) for space nomenclature/ directions. • Plastering with cement mortar 1:5 (1 cement: 5 sand) of 12 mm thick in interior face of the walls and concrete columns including hacking the concrete surface brushing, scaffolding, curing and surface shall be smooth trowel finish as per standard specification. • Anti-termite treatment of the entire critical area

5.13.6 Non- IT –Electrical work Guidelines and Specifications

S. No.	Component	Guidelines / Specifications
1.	PVC Conduit	<ul style="list-style-type: none"> • The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for nonmetallic conduit 1.6 mm thick as per IS 9537/1983. • All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables. • No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit. • All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly. • Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted

		<p>between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.</p> <ul style="list-style-type: none"> • Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal. • The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm Centre the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.
2.	Wiring	<ul style="list-style-type: none"> • PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed. • Looping system of wiring shall be used, wires shall not be jointed. No reduction of strands is permitted at terminations. No wire smaller than 3.029 sq.mm. shall be used. • 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 used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit. • Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply. • Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other. • 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.

		<ul style="list-style-type: none"> • All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one. • Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts. The earth continuity insulated copper wire in Green color shall be run inside the conduit to earth the third pin or socket outlets, earth terminal of light fixtures, fan etc. as required. Lights points shall be either of single control, twin control or multiple points controlled by a single switch / MCB as per scheduled of work. Bare copper wire shall be provided with each circuit from DB as specified in the item of work and terminated in earth bar of DBs and switch boxes with proper lugs as required maximum number of PVC insulated 650 / 1100 grade copper conductor cable which can be drawn in a conduit.
3.	Earthing	<p>All electrical components are to be earthen is to by connecting two earth tapes from the frame of the component ring will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthing shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS- 3843-1986. The entire applicable IT infrastructure in the Data Centre shall be earthed.</p> <ul style="list-style-type: none"> • Earthing should be done inside the Data Centre for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units etc. to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits. • All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded. • The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment. • Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.

		<ul style="list-style-type: none"> • The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room. • There should be enough space between data and power cabling and there should not be any cross wiring of the two, to avoid any interference, or corruption of data. • The earth connections shall be properly made. A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings. • The DCO would be responsible for providing separate Earthing for Servers, UPS & Generators as per the standards
4.	Cable Work	<ul style="list-style-type: none"> • 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 crisis crossing is avoided and final take off to switch gear is easily facilitated. • All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick aluminum strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported 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 earthing 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 crisscross wiring of the two, to avoid any interference, or corruption of data
5.	Electrical Panels	<ul style="list-style-type: none"> • The Panels shall be of compartmentalized design so that circuit arc / flash products do not create secondary faults and be fabricated out of high quality CRCA sheet, suitable for indoor installation having dead front operated and floor mounting type. • All CRCA sheet steel used in the construction of Panels shall be 2 mm. thick and shall be folded and braced as necessary to provide a rigid support for all components. Joints of any kind in sheet steel shall be seam welded, all welding slag grounded off and welding pits wiped smooth with plumber metal. • The Panels shall be totally enclosed, completely dust and vermin proof and degree of protection being not less than IP: 54 to IS: 2147. Gaskets between all adjacent units and beneath all covers shall be provided to render the joints dust proof. All doors and covers shall be fully gasketed with foam rubber and /or rubber strips and shall be lockable. • All panels and covers shall be properly fitted and secured with the frame and holds in the panel correctly positioned. Fixing screws shall enter into holes, taped into an adequate thickness of metal or provided with bolts and nuts. Self-threading screws shall not be used in the construction of Panels. • A base channel of 75 mm. X 50 mm. X 6 mm. thick shall be provided at the bottom. • Panels shall be preferably arranged in multi-tier formation. The size of the Panels shall be designed in such a way that the internal space is sufficient for hot air movement. If necessary, openings shall be provided for natural ventilation, but the said openings shall be screened with fine weld mesh. The entire electrical component shall be derated for 50°C. • The Panels shall be provided with removable sheet steel plates at top and bottom to drill holes for cable / conduit entry at site. • The Panels shall be designed to facilitate easy inspection, maintenance and repair. • The Panels shall be sufficiently rigid to support the equipment without distortion under normal and under short circuit condition. They shall be suitably braced for short circuit duty <p>Circuit Compartments</p> <ul style="list-style-type: none"> • Each MCCB shall be housed in separate compartments and shall be enclosed on all sides. Sheet steel hinged lockable door shall be duty interlocked with the unit in 'ON' and 'OFF' position.

		<ul style="list-style-type: none"> • All instruments and indicating lamp shall be mounted on the compartment door. Sheet steel barriers shall be provided between the tiers in a vertical section. <p>Instrument Compartments</p> <ul style="list-style-type: none"> • Separate adequate compartment shall be provided for accommodating instruments, indicating lamps, control contactors/ relays and control fuses etc. • These components shall be accessible for testing and maintenance without any danger of accidental contact with live parts, bus bar and connections <p>Busbars</p> <ul style="list-style-type: none"> • The busbar shall be air insulated and made of high quality, high conductivity, high strength Aluminum. • The busbar shall be of 3 phases and neutral system with separate neutral and earth bar. The size of neutral busbar in all main panels or lighting panels and feeders for panel shall be equal to phase busbar. • The busbar and interconnection between busbars and various components shall be of high conductivity Aluminum. • The busbar shall be of rectangular cross-section designed to withstand full load current for phase busbars and half rated current for neutral busbars in case of MCC panels only and shall be extensible on either side. • The busbar size shall be as per the rating of the panel. The busbar shall have uniform cross-section throughout the length. • The busbars and interconnections shall be insulated with epoxy-coated busbar. The busbar shall be supported on bus insulators of non-flammable type with high creepage and high anti tracking property and non-hydroscopic SMC / DMC insulated supports at sufficiently close intervals to prevent busbars sag and shall effectively withstand electromagnetic stresses in the event of short circuit. • The busbar shall be housed in a separate compartment. The busbar shall be isolated with 3-mm. thick Bakelite sheet to avoid any accidental contact. The busbar shall be arranged such that minimum clearance between the busbar are maintained as below: <ul style="list-style-type: none"> ○ Between phases: 25 mm. minimum ○ Between phases and neutral: 25 mm. ○ Between phases and earth: 25 mm. ○ Between neutral and earth: 20 mm. minimum
--	--	--

		<ul style="list-style-type: none"> • All busbar connections shall be done by drilling holes in busbars and connecting by chromium plated or tinned plated brass bolts and nuts. • Additional cross-section of busbar shall be provided in all Panels to cover up the holes drilled in the busbar. Spring and flat washers shall be used for tightening the bolts. • All connections between busbars and circuit breakers / switches and cable terminals shall be through aluminum strips of proper size to carry full rated current. These strips shall be insulated with insulating taps. • Panel to panel entry of bus bar shall be effectively sealed by electrical and thermal insulation barriers so that products of flashover do not travel from one panel to another panel creating multiple faults. • Busbar calculated on 50 deg. C. ambient temp. and 85 deg. C. for continuous and short time rating. Busbar surrounded air temp. shall be considered 70 deg. C. for busbar calculation • All joint shall have non-flammable insulation shrouds for secondary insulation purpose <p>Electrical Power and Control Wiring Connection</p> <ul style="list-style-type: none"> • Terminal for both incoming and outgoing cable connections shall be suitable for 1100 V grade, aluminum / copper conductor XLPE insulated and PVC sheathed, armored cable and shall be suitable for connections of solder less sockets for the cable size as per the feeder capacity. • Power connections for incoming feeders of the main Panels shall be suitable for 1100 V grade aluminum conductor (XLPE) cables. • Both control and power wiring shall be brought out in cable alley for ease of external connections, operation and maintenance. • Both control and power terminals shall be properly shrouded. • 10% spare terminals shall be provided on each terminal block. Sufficient terminals shall be provided on each terminal block, so that not more than one outgoing wire is connected to per terminal. • Terminal strips for power and control shall preferably be separated from each other by suitable barriers of enclosures. • Wiring inside the modules for power, control, protection and instruments etc. shall be done with use of 660 / 1100 V grade, FRLS insulated copper conductor cables conforming to IS. For
--	--	--

		<p>current transformer circuits, 2.5 sq.mm. copper conductor wire shall be used.</p> <ul style="list-style-type: none"> • Other control wiring shall be done with 1.5 sq.mm. copper conductor wires. • Wires for connections to the door shall be flexible. All conductors shall be crimped with solder less sockets at the ends before connections are made to the terminals. • Control power supply to modules through the control transformer Control power wiring shall have control fuses, (HRC fuse type) for circuit protection. All indicating lamps shall be protected by HRC fuses. • Care shall be taken to ensure that the layout of wiring is neat and orderly. Identification ferrules shall be filled to all the wire termination for ease of identification and to facilitate checking and testing <p>Terminals</p> <ul style="list-style-type: none"> • The outgoing terminals and neutral link shall be brought out to a cable alley suitably located and accessible from the panel front. • The current transformers for instruments metering shall be mounted on the disconnecting type terminal blocks. • No direct connection of incoming or outgoing cables to internal components of the distribution board is permitted; only one conductor may be connected in one terminal <p>Cable Compartments</p> <ul style="list-style-type: none"> • Cable compartments of minimum 300 mm size shall be provided in the Panels for easy termination of all incoming and outgoing cables entering from bottom or top. • Adequate supports shall be provided in the cable compartments to support cables. • All outgoing and incoming feeder terminals shall be brought out to terminals blocks in the cable compartment. <p>Labels</p> <ul style="list-style-type: none"> • Engraved PVC labels shall be provided on all incoming and outgoing feeders.
--	--	---

	<ul style="list-style-type: none"> • Single line circuit diagram showing the arrangements of circuit inside the distribution board shall be pasted on inside of the panel door and covered with transparent laminated plastic sheet. <p>Name Plates</p> <ul style="list-style-type: none"> • A nameplate with the Panels designation in bold letters shall be fixed at top of the central panel. • A separate nameplate giving feeder details shall be provided for each feeder module door. • Inside the feeder compartments, the electrical components, equipment's, accessories like switchgear, control gear, lamps, relays etc. shall suitably be identified by providing stickers. • Engraved nameplates shall preferably be of 3 ply, (Red-White-Red or Black-White-Black) lamicold sheet. However, black engraved perplex sheet name plates shall also be acceptable. Engraving shall be done with square groove cutters. • Nameplate shall be fastened by counter sund screws and not by adhesives <p>Danger Notice Plates</p> <ul style="list-style-type: none"> • The danger notice plate shall be affixed in a permanent manner on operating side of the Panels. • The danger notice plate shall indicate danger notice both in Hindi and English and with a sign of skull and bones. • The danger notice plates, in general, meet the requirements of local inspecting authorities. • Overall dimensions of the danger notice plate shall be 200 mm. wide X 150 mm. high. • The danger notice plate shall be made from minimum 1.6 mm. thick mild steel sheet and after due pre-treatment to the plate, the same shall be painted white with vitreous enamel paint on both front and rear surface of the plate. • The letters, the figures, the conventional skull and bones etc. shall be positioned on plate as per recommendation of IS: 2551-1982. • The said letters, the figures and the sign of skull and bones shall be painted in signal red color as per IS: 5-1978. • The danger plate shall have rounded corners. Location of fixing holes for the plate shall be decided to suit design of the Panels.
--	--

	<ul style="list-style-type: none"> • The danger notice plate, if possible, it should be of ISI certification mark <p>Molded Case Circuit Breakers</p> <ul style="list-style-type: none"> • The molded case circuit breaker (MCCB) shall be air break type and having quick make - quick break with trip free operating mechanism. • Housing of the MCCB shall be of heat resistant and flame retardant insulating material. • Operating handle of the MCCB shall be in front and clearly indicate ON/OFF/TRIP positions. • The electrical contact of the circuit breaker shall be of high conducting non-deteriorating silver alloy contacts. • The MCCB shall be provided microprocessor based overload and short circuit protection device. • All the releases shall operate on common trip busbar so that in case of operation of any one of the releases in any of the three phases, it will cut off all the three phases and thereby single phasing of the system is avoided. • The MCCB shall provide two sets of extra auxiliary contacts with connections for additional controls at future date. <p>Contactors</p> <ul style="list-style-type: none"> • The contactors shall meet with the requirements of IS: 2959 and BS: 7755. • The contactors shall have minimum making and breaking capacity in accordance with utilization category AC3 and shall be suitable for minimum Class II intermittent duty. • If the contactor forms part of a distribution board then a separate enclosure is not required, but the installation of the contactor shall be such that it is not possible to make an accidental contact with live parts <p>Indicating Lamps</p> <ul style="list-style-type: none"> • Indicating lamps assembly shall be screw type with built in resistor having non-fading color lens. LED type lamps are required. • Wiring for Remote ON, OFF, TRIP indicating lamp is required.
--	---

		<ul style="list-style-type: none"> • Color shade for the indicating lamps shall be as below: <ul style="list-style-type: none"> o ON indicating lamp: Red o OFF indicating lamp: Green o TRIP indicating lamp: Amber o PHASE indicating lamp: Red, Yellow, Blue o TRIP circuit healthy lamp: Milky
--	--	---

5.13.7 General Guidelines for Data Centre

- I. All the hardware specifications mentioned in the RFP are the required minimum, higher or better specifications would be acceptable.
- II. Component furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such component's and/or needed for erection, completion and safe operation of the components as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions. All similar standard components/parts of similar standard components provided shall be inter-changeable with one another.
- III. The methodology of cabling and installation work to be adopted for the Data Centre shall ensure minimum damage to the existing structure of the building. Any damage to the existing flooring/walls/paint etc. shall be made good by the selected bidder. It is advised that bidder should visit site before submitting the tender to get apprised about the site conditions.
- IV. The MSI shall be responsible for providing all materials, components, and services, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability, and reliability of the complete component covered under this specification within his quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract.
- V. The MSI shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the MSI.
- VI. The MSI shall perform the services and carry out its obligations with all due diligence, efficiency and economy in accordance with generally accepted professional techniques and practices and shall observe sound management practices and employ appropriate advance technology and safe methods.
- VII. The MSI shall furnish complete, well-fabricated and reliably operating and secure systems to SDA. Design and selection of component and software shall be consistent with the requirements of long term trouble free operation with highest degree of reliability and maintainability. All components shall be constructed to operate safely without undue heating, vibration, wear, corrosion, electromagnetic interference or similar problems and all software shall be proven, tested and reliable.
- VIII. All interconnecting cables required to connect the communication component shall be furnished. All cables shall be fully assembled connector pre-terminated and factory tested as part of overall system checkout. Cables shall be neatly & properly tied up and dressed using appropriate cable hangers and Velcro bands. All the cables, connectors, sockets, panels etc. shall be labelled for identification purpose.
- IX. All the cabling should adhere to the TIA-942 Data Centre Standard.

-
- X. All component, accessories and cables supplied under this contract shall be in accordance with the latest applicable recommendations, regulations and standards of:
- a. CCITT/ITU
 - b. ANSI
 - c. IEC 60364
 - d. IEEE Standard 1100
 - e. IETF
 - f. TIA 942
 - g. ISA 3043
 - h. EIA/TIA 568 Standards
 - i. NFPA 72 and NFPA 318
 - j. International Electro-Technical Commission (IEC)
 - k. Cable (Cat 6) and cable accessories (Cat6) UL Listed and verified
- XI. For parameters not covered under the above codes, internationally acceptable standards shall be accepted. The MSI shall furnish a complete list of all standards and codes under which his component is designed, manufactured and assembled along with the bids.
- XII. Functionality/accessibility of each component of the system and the system as a whole should be demonstrated to the satisfaction of ASCL.

6 Annexure II: Technical Specifications Hardware

6.1 City Surveillance

6.1.1 Standard GI Pole

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Requirement	Shall be minimum 20 feet (6.5 meter) height as per NHA norms	
2.	General Requirement	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate size 30x30x15 cm suitable for wind speed 50m/sec with suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980)	
3.	Foundation	The pole would be fixed on an adequate and strong foundation to withstand city weather conditions and wind speed of 150km / hr	
4.	Foundation	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100 cm or better	
5.	Protection	Lighting arrestors with proper grounding	
6.	Sign Board with number plate	Sign board depicting the area under surveillance and with the serial number of the pole	
7.	Height	The height of the pole shall be as per requirement of the location varying from 6.5 meters to 15 meters.	

6.1.2 Cantilever GI Pole

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Requirement	Shall be minimum 6 meters. height as per NHA norms Overhang: 9 meters. or 6 or 3 meters depending on lanes	
2.	Quality	Mild Steel (M.S) Tubular Pipe (B-Class) as per IS-1239 (Part-1)-193	
3.	Base Plate	Size 400 mm X 400 mm X 16 mm thick welded to the bottom of the signal pole	
4.	Foundation	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100 cms. or better <ul style="list-style-type: none"> • Length: 600 mm • Width: 600 mm 	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> Depth: 150 mm Bolts: 25 mm/8 Nos. 8 mm Rings: 8 Nos. 16 mm Rods: 12 Nos. 	
5.	Protection	Lighting arrestors with proper grounding	
6.	Sign Board with number plate	Sign board depicting the area under surveillance and with the serial number of the pole	
7.	Paint	Pole painted with two coats of primer and in addition bituminous painting for other bottom 1.5 m portion of pole	
8.	Arms	The pole shall be able to support 2 arms of 6-meter length each on either side and suitable for ANPR and Surveillance camera mounting	

6.1.3 Fixed Box Outdoor Camera - Face recognition, ANPR and General Surveillance

These fixed box cameras shall be installed outdoors for face recognition for e.g. at crime hotspots, for ANPR at critical transit hubs and City entry and exit points and general surveillance in the city.

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Image Sensor	Minimum 1/2.8" progressive scan RGB CMOS	
2.	Operating Frequency	50/60 Hz	
3.	Day/ Night Operation	With IR Cut Filter	
4.	Minimum Illumination	Colour: 0.2 Lux @ 25/30 IRE B/W: 0.01 @ 25/30 IRE 0 Lux with Built in or External IR, IR Range 100 Meters	
5.	Low light Capability	The camera shall be able to provide usable Colour video in low light conditions	
6.	Lens	5-50/9-40 mm IR corrected, CS-mount/Built-in lens, P-Iris	
7.	Electronic Shutter	1/30 to 1/8000 s or better	
8.	Image Resolution	1920 X 1080, 1280 X 720, 800 X 450	
9.	Compression	H.265/H.264 compression with 3 Mbps and lower bitrate at 1920 X 1080 @ 30 FPS per stream	
10.	Frame Rate and Bit Rate	25/30 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit.	
11.	Video Streams	The camera shall be able to setup and stream out minimum two (2) stream profiles. It should be possible to set each stream profile independently for compression, resolution, frame rate and quality up to Full camera resolution of Full HD @ 30 FPS	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
12.	Motion Detection	Built in with multiple configurable areas in the video stream	
13.	Electronic Exposure & Control	Automatic/ Manual	
14.	Wide Dynamic Range	90 dB or better	
15.	Backlight Compensation	Required	
16.	Privacy Masks	Minimum 4 configurable 3D zones	
17.	Connectors	1 Input & 1 Output for Alarm Interface	
18.	Audio	Two-way Audio	
19.	Event Triggers	Intelligent video, Edge Storage event, External Input Motion Detection, Day/Night Mode, Network, Time scheduled, 3rd Party Analytics, Manual Trigger, Alarm Input Trigger	
20.	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP, Edge Storage/ NAS Storage, Pre- & Post Alarm Recording, Actions configurable by web interface, External Output activation	
21.	Edge Storage	SD Card Slot with minimum 64 GB Class 10 SD card and expansion 128 GB	
22.	Remote Focus	Ability to fine tune focus of camera remotely	
23.	Protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP, SMTP, UPnP™, SNMPv1/v2c/v3 (MIB - II), DNS NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP	
24.	Text Overlay	Date & time, and a customer-specific text, camera name etc.	
25.	Security	Password protection, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log	
26.	Firmware Upgrade	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost	
27.	Logs	The camera shall provide minimum logs of latest connections, access attempts, users connected, changes in the cameras etc.	
28.	Interface	RJ 45, 100 Base TX	
29.	Enclosure	IP66/NEMA 4X casing made of Polycarbonate/Aluminium, IK 08 or above	
30.	Power requirements	PE IEEE 802.3af / POE+ IEEE 902.3at compliant	
31.	Operating Temperature	-10 °C to 50 °C	
32.	Operating Humidity	Humidity 20–90% RH (non-condensing)	
33.	Certification	UL, CE, FCC, IEC	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
34.	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost	
35.	Housing, Mount and IR	Shall be of the same make of OEM or better	
36.	Onvif S	Required	
37.	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS	
38.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features	
39.	White Balance	Auto and Manual setting	
40.	Support	The system should not be an end of life / end of service product	
41.	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.	
42.	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols	

6.1.4 Bullet Indoor Camera - Face recognition

These bullet cameras shall be installed at Airport, Railway and Bus Station Entry and Exit Gates.

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Image Sensor	Minimum 1/3" progressive scan RGB CMOS or better	
2.	Operating Frequency	50/60 Hz	
3.	Day/ Night Operation	With IR Cut Filter	
4.	Minimum Illumination	Colour: 0.3 Lux @ 30 IRE F1.4; 0 Lux with Built in or External IR, IR Range 30 Meters	
5.	Mechanical Pan Tilt Adjustment	Pan: $\pm 135^\circ$, Tilt: $0^\circ - 90^\circ$	
6.	Lens	3 - 9 mm, IR corrected, P-Iris, Megapixel Lens with remote zoom and focus	
7.	Electronic Shutter	1/30 s to 1/8000 s or better	
8.	Image Resolution	1920 X 1080 or better	
9.	Compression	H.265/H.264 compression with 3 Mbps and lower bitrate at 1920 X 1080 @ 30 FPS per stream	
10.	Frame Rate and Bit Rate	Up to 25/30 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit	
11.	Video Streams	The camera shall be able to setup and stream out minimum two (2) stream profiles. It should be possible to set each stream profile independently for compression,	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		resolution, frame rate and quality up to Full camera resolution of Full HD @ 25/30 FPS	
12.	Motion Detection	Built in with multiple configurable areas in the video stream	
13.	Image Configuration	The Camera shall be able to Include or Exclude any area of any size/ dimension within the scene in order to eliminate false alarm and also optimize the bandwidth and storage	
14.	Wide Dynamic Range	90 dB or better	
15.	Backlight Compensation	Required	
16.	IR	30 Meter (Built in or External) Optimized IR with adjustable intensity and angle	
17.	Event Triggers	Live Stream Accessed, Motion Detection, Network, Temperature, Camera Tampering, Edge Storage Disruption, Video Analytics, Manual Trigger	
18.	Event Actions	FTP, HTTP, network share, email Notification: email, PTZ function, Edge Storage/ NAS Storage, Pre- & Post Alarm Recording, Actions configurable by web interface, WDR Mode, External Output Trigger, Text Overlay	
19.	Edge Storage	SD Card Slot with minimum 64 GB Class 10 SD card and expansion 128 GB	
20.	Protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP SMTP, Bonjour, UPnP, SNMPv1/v2c/v3 (MIB - II), DNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP SSH	
21.	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.	
22.	Security	Password protection, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log	
23.	Firmware Upgrade	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost	
24.	Interface	RJ 45, 100 Base TX	
25.	Enclosure	IP66 /NEMA-4X-rated casing Polycarbonate/Aluminium, IK 08 or above	
26.	Power requirements	PE IEEE 802.3af / POE+ IEEE 902.3at compliant	
27.	Operating Temperature	-10 °C to 50 °C	
28.	Operating Humidity	Humidity 20–90% RH (non-condensing)	
29.	Certification	UL, CE, FCC, IEC	
30.	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain	
31.	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
32.	Mount	Wall Mount/ Pole Mount	
33.	Onvif S	Required	
34.	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS	
35.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features	
36.	White Balance	Auto and Manual setting	
37.	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.	
38.	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols	

6.1.5 360 Degree Panoramic Multi-Sensor Camera

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Image Sensor	4 X 1/2.8" progressive scan CMOS or better	
2.	Operating Frequency	50/60 Hz	
3.	Day/ Night Operation	Built-in Automatic IR Cut Filter	
4.	Minimum Illumination	Colour: 0.3 Lux @ 30 IRE	
5.	Lens	F= 2.8–8 mm, remote focus, remote zoom	
6.	Field of View	Remotely Adjustable	
7.	Electronic Shutter	1/8000 s to 1/25	
8.	Image Resolution	4 X 1920 X 1080 (1080p)	
9.	Compression	H.265/H.264 compression with 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream	
10.	Frame Rate and Bit Rate	Shall support up to 30 fps	
11.	Video Streams	The camera shall be able to setup and stream out minimum eight (4X2=8) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently up to Full HD @ 30 FPS	
12.	Motion Detection	Built in with multiple configurable areas in the video stream	
13.	Image settings	Saturation, contrast, brightness, sharpness, WDR, white balance, exposure control, exposure zone, fine tuning of behaviour at low light, text and image overlay, privacy mask, compression	
14.	Intelligent capabilities	Live Stream Accessed, Motion Detection, Network, Active Tampering, Edge Storage Disruption, 3rd Party Analytics, Manual Trigger, Virtual Input, Built in pixel counter	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
15.	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and Overlay text, pre- and post-alarm video buffering, SNMP trap	
16.	Edge Storage	SD Card Slot with minimum 128 GB Class 10 SD card	
17.	Storage	Support for recording to dedicated network-attached storage	
18.	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera	
19.	Protocols	IPv4/v6, HTTP, HTTPS, SSL/TLS, 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	
20.	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.	
21.	Security	Password protection, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log, Centralized Certificate Management	
22.	Firmware Upgrade	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost	
23.	Logs	The camera shall provide logs of latest connections, access attempts, users connected, changes in the cameras etc.	
24.	Interface	RJ 45, 100 Base TX	
25.	IR illumination	External/Internal IR illumination up to distance of 30 meters from camera	
26.	Enclosure	IP66/NEMA 4X, IK08 impact-resistant aluminium or plastic casing with polycarbonate hard-coated dome	
27.	Power requirements	Power over Ethernet (PoE) IEEE 802.3af/802.3at	
28.	Operating Temperature	-10 °C to 50 °C	
29.	Operating Humidity	20–90% RH (condensing)	
30.	Certification	UL, CE, FCC, IEC, EN	
31.	Application Programmers Interface	The camera shall be fully supported by an open and published using web service RESTAPI (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications	
32.	Mount	Wall/ Ceiling/ Surface/ Pole	
33.	Onvif S	Required	
34.	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS	
35.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features	
36.	White Balance	Auto and Manual setting	
37.	Support	The system should not be an end of life / end of service product	

6.1.6 PTZ Camera

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols	
2.	Image Sensor with WDR	True WDR 90 db or better, 1/2.8" Progressive CMOS Sensor or better with minimum 2 MP resolution	
3.	Resolution	Camera should be Full HD PTZ 1920 (w) x1080 (h)	
4.	Frame Rate	Shall support up to 25/30 fps	
5.	Lens specs	Auto-focus, 4.4 –120mm (corresponding to 25x) or better	
6.	Minimum illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE) or better	
7.	Pre-set Positions	256 or better, Pre-set tour	
8.	PTZ	Pan: 0 to 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 20x optical zoom and 10x digital zoom	
9.	General	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently	
10.	Outdoor Protection	The camera should be complete with IP 66 rated housing, Connectors, Camera Mounts, Power Supply and all Ancillary Equipment & all accessories	
11.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, 802.1X, IPv4/v6, QoS, DNS, DDNS, NTP	
12.	Compression Capability	H.265/H.264 compression with 3 Mbps and lower bitrate at 1920 X 1080 @ 30 FPS per stream and MJPEG	
13.	Noise Reduction	DNR (2D/3D)	
14.	Certificate	CE, UL, FCC, ONVIF	
15.	Industry Standards	ONVIF S Compliant	
16.	Miscellaneous	Power Supply: External 12V /24V/48V DC/ POE+	
17.	Ethernet	Connectors: 10Base-T/100Base-TX	
18.	Miscellaneous	Cable routing through base or rear of housing or feed through	
19.	Miscellaneous	Operating conditions unit: -10° C to 50° C or better, humidity 20% to 90% non-condensing	
20.	Miscellaneous	Tamper Proof	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
21.	Miscellaneous	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS	
22.	Audio	Audio capture Capability	
23.	Local Storage	SD Card Slot with minimum 64 GB Class 10 SD card and expansion 128 GB	
24.	Security	Password Protection, HTTPS encryption, IEEE 802.1X	
25.	S/N Ratio	≥ 50dB	
26.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features	
27.	Mounting Accessories	For pole and surface mount with L/C Brackets	
28.	IR Illumination	Internal/External > 150 meters	

6.1.7 Public Address System with Integrated Audio Amplifier

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> The system should allow streaming in both local network and internet and operable from Central command centre. System should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all location (1: many) simultaneously. The PAS should also support both, Live and pre-recorded inputs Unlimited number of both sources and incomers of stream in the system Division of the speakers into independently controlled groups, minimum 2 Speaker, to be used for public address system at a location. Possibility to setup an independent operating Audio playback from a file or an external source Audio streams mixing - playlist creation support 	
2.	Audio	<ul style="list-style-type: none"> One-way/two-way (mono) 	
3.	Compression	G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, WAV, MP3 in mono/stereo from 64 kbps to 320 kbps. Constant and variable bit rate. Sampling rate from 8 kHz up to 48 kHz. Configurable bit rate	
4.	input/output	Built-in microphone with frequency 50 Hz - 16 kHz (for testing purpose)	
5.	Max sound pressure level	>120 dB	
6.	Frequency response	280 Hz -12.5 kHz	
7.	Coverage	Minimum 70° horizontal by 95° vertical (at 2 kHz)	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
8.	Built In Amplifier	7 W Class D amplifier	
9.	Security	Password protection, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log	
10.	Supported protocols	IPv4/v6, HTTP, HTTPS, SIP, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP, SOCKS, SSH	
11.	Audio functionality	The horn speaker shall support SIP for integration with VoIP, peer-to-peer or integrated into SIP/PBX	
12.	Language	The horn speaker shall provide a function for altering the language of the user interface, and shall include support for at least English and Hindi	
13.	Installation and Maintenance	The horn speaker shall include a test functionality allowing a test tone sequence to be generated and measured by the built-in microphone to verify full functionality	
14.	API	Horn speakers shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications	
15.	Firmware	The firmware upgrade shall be done through web interface, the firmware shall be available free of cost	
16.	Audio Speaker test	Shall be available for testing speaker functionality	
17.	Event triggers	Call, Virtual inputs	
18.	Event actions	<ul style="list-style-type: none"> • File upload via HTTP/network share/ email • Notification via email, HTTP and TCP • Play audio clip • Send Auto Speaker Test • Send SNMP trap • Status LED 	
19.	Built-in installation aids	Test tone	
20.	Functional monitoring	Auto Speaker Test, Connection verification, Built-in system logging	
21.	Housing	Impact-resistant aluminium, IP66 rated	
22.	Built in Memory	Minimum 256 MB RAM, 256 MB Flash	
23.	Power	Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3(max 14 W)	
24.	Connectors	RJ45 10BASE-T/100BASE-TX PoE	
25.	Operating Temperature	0°C to 50 °C	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
26.	Operating Humidity	Humidity 10–100% RH (condensing)	
27.	Certification	EN, CE, FCC, UL, IEC	

6.1.8 IR illuminator

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range Distance	Minimum 100 Meters	
2.	Adaptive illumination	10 to 80 degrees using lens; High sensitivity at Zero lux	
3.	Power	Input 100-240V AC, or 12/24 V AC/DC, and automatic on/off operation	
4.	Casing	IP66 rated / NEMA 4X vandal resistance	
5.	Operating Condition	-5° to 55°C or better	
6.	Certification	CE, FCC, RoHS	
7.	Lighting	LED's	
8.	Required Accessories	Power Supply, Mounting Clamps, U-bracket	

6.1.9 Emergency Call Box with Panic Button

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Function	The two-way call should be automatically established from the Emergency call box to ICCC Police Helpdesk or other location as provided by police with Live Video Streaming from Emergency call box camera capturing the live situation and emergency caller. There should be featuring to terminate the call from both ends.	
2.	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment	
3.	Call Button	Watertight Push Button, Visual Feedback for button press	
4.	Speaker & Microphone	VOIP Phone, Hands-free calling, Watertight and industrial grade equipment, Built-In minimum 8 Ohm Speaker with minimum 20W Class D amplifier	
5.	Connectivity	3G/4G/Ethernet/Fiber as per solution offered	
6.	CCTV Camera	IP based, Color camera with minimum D1 resolution, Day/Night mode operations	
7.	Battery	Internal Battery with different charging options (Solar/Mains)	
8.	Power	Automatic on/off operation	
9.	Casing	IP-65 rated for housing	
10.	Operating Conditions	0° to 50°C	
11.	Certification	UL/CE/EN	

6.1.10 ANPR LPU (Inside Junction Box)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Technical	Shall have minimum Quad Core CPU (4 physical CPU cores)	
2.	Technical	Shall have minimum 64-bit architecture	
3.	Technical	Shall have minimum 8 GB RAM (DDR3-1600 or above)	
4.	Technical	Shall have minimum 500 GB Hard Disk	
5.	Technical	Shall have Dedicated Gigabit network port per camera (Maximum Transmission Unit 9000 / jumbo frames), +1 LAN port	
6.	Technical	Shall have capability to connect 4 cameras per LPU	

6.1.11 Body Camera with Docking System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The Body Worn Camera System (BWCS) should consist of a single device comprising of a camera, rechargeable battery and recording unit. It should be able to capture clear high definition video & audio as well as take still photographs. It should be able to compress the video/audio files using appropriate non-proprietary algorithm and store it on a local drive.	
2.	Dimensions	The BWCS should be lightweight, of a small size and be comfortable to wear on the body. It can be mounted / installed on the shoulder or shirt front or shirt pocket etc. The mounting should be of an ambidextrous design and should keep the equipment stable.	
3.	Capture of video, audio and still photographs	The BWCS should be a point of view audio/video recording system capable of capturing audio/video/still photographs of what the officer is seeing.	
4.	Date and Time Stamping	The camera shall contain an embedded real-time clock which provides accurate date and time stamps on videos/ photographs.	
5.	Recording Resolution	The camera should encode video at resolution up to HD quality (1280 X 720 pixels or better).	
6.	Camera Sensor	The camera should capture video & photograph with a minimum of 1-megapixel sensor. It should also have capability of night mode recording.	
7.	Field of view of lens	100 degrees or better.	
8.	Display	Minimum 2" LCD colour Display	
9.	Replay	The device should be able to play the recorded audio/video/images on the screen.	
10	Compression	The camera must support MPEG-4 / H.264 (video) and MPEG-4/ MP2 (audio) compression algorithm and should offer the compression at up to 30 frames per second.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
11	Storage	The BWCS shall support on-board storage via Solid State Storage or SD Card of 32 GB capacity (included). The on-board storage should be sufficient to record up to 08 hours at maximum resolution.	
12	Battery	The BWCS should be supplied with an internal rechargeable Lithium battery. The battery should be of appropriate capacity to allow for continuous use including recording for up to 4 hours.	
13	Battery recharge time	The battery recharge time from empty to full capacity should be not more than 3 hours.	
14	Data Transfer	Each BWCS should be able to connect and upload data using a USB 2.0 port or better.	
15	Configurations and Video Management	All configurations (including the adjustment of the real-time clock) of the BWCS should be possible via a PC-based windows application. The management application should allow the user to backup and transfer data from one or multiple BWCS and allow query for video/photograph on the basis of device, user, time, filename etc.	
16	Battery charger	Each BWCS should be supplied with a separate charger.	
17	Security features	The user should not be able to delete / edit / overwrite original video file/photograph. The deletion/uploading/ transfer of video/photograph on a PC should be possible only through the management software and should be administrator controlled. However, there should be an option of auto-overwriting based on oldest-file-first-to-be-deleted, once the memory is full and further recording is being done.	
18	Design	The BWCS should be water resistant, dust resistant, and impact resistant and should be operable in normal steady rainfall (IP-66 or better). The BWCS should have an LED warning light which should remain 'On' when the camera is recording. It should also give an audible beep when the camera is switched on/ off and when the battery has become low etc.	
19	Operating Temperature	0 to 55 degrees C.	
20	Night Vision	The body camera shall be able to stream live video to VMS and recording server over 4G/LTE	
21	GPS	The body camera shall integrate ICCC Platform to show real-time location	
22	Capacity of Docking System	Min 10 slot chassis with battery charging	
23	Connection: Docking System	Single USB and Power connection	
24	Functionality for Docking System	Should be Capable to transfer data from device automatically to defined system when docked and	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		simultaneously charge the device. Docking station for single device and 10 (for multiple device data transfer and charging at a time) both to be provided	

6.2 Environment Sensor

6.2.1 Air Quality Monitoring Station

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Should be ruggedized enough to be deployed in open air areas, on streets and parks	
2.	General	Should be able to read and report the following parameters: PM 10, PM 2.5, NO2, SO2, CO, O3, CO2,	
3.	Connectivity	Sensors should be able to connect through Fibre, USB, Ethernet, Wi-Fi, 2G, 3G 4G, LTE, LoRA connectivity mediums, whichever was feasible	
4.	Environmental Conditions	Enclosure shall be rugged weather proof IP65 rated and shall house the power modules, thermal management system, embedded PC and user configured analyzer modules as well	
5.	Environmental Conditions	Environmental operating range shall be 0°C to +60°	
6.	General	The design shall be modular in nature which shall have the capability to add additional environmental sensors in the future into the enclosure	
7.	General	Data of all the environmental sensor shall be available on the same software interface	
8.	General	It shall be possible to remove or replace individual sensor modules without affecting the functioning of rest of the system	
9.	General	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod stand or a standalone pole	

6.2.2 Carbon Mono Oxide (CO) Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	Range of CO sensor shall be between 0 to 1000 PPM	
2.	Resolution	Resolution of CO sensor shall be 0.01 PPM or better	
3.	Lower Detectable Limit	Lower detectable limit of CO sensor shall be 0.040 PPM or better	
4.	Precision	Precision of CO sensor shall be less than 3% of reading or better	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Linearity	Linearity of CO sensor shall be less than 1% of full scale or better	
6.	Response Time	Response time of CO sensor shall be less than 60 seconds	
7.	Operating Temperature	Operating temperature of CO sensor shall be 0°C to 60°C	
8.	Operating Pressure	Operating pressure of CO sensor shall be $\pm 10\%$	

6.2.3 Ozone (O3) Sensor

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	O3 Sensor shall have a range of at least 0-1000 PPB.	
2.	Resolution	Resolution of O3 sensor shall be 10 PPB or better.	
3.	Lower Detectable Limit	Lower detectable limit of O3 sensor shall be 10 PPB or better.	
4.	Precision	Precision of O3 sensor shall be less than 2% of reading or better.	
5.	Linearity	Linearity of O3 sensor shall be less than 1% of full scale.	
6.	Response Time	Response time of O3 sensor shall be less than 60 seconds.	
7.	Operating Temperature	Operating temperature of O3 sensor shall be 0°C to 60°C.	
8.	Operating Pressure	Operating pressure of O3 sensor shall be $\pm 10\%$.	

6.2.4 Nitrogen Dioxide (NO2) Sensor

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	NO2 Sensor shall have a range of at least 0-10 PPM.	
2.	Resolution	Resolution of NO2 sensor shall be 0.001 PPM or better.	
3.	Lower Detectable Limit	Lower detectable limit of NO2 sensor shall be 0.001 PPM or better.	
4.	Precision	Precision of NO2 sensor shall be less than 3% of reading or better.	
5.	Linearity	Linearity of NO2 sensor shall be less than 1% of full scale.	
6.	Response Time	Response time of NO2 sensor shall be less than 60 seconds.	
7.	Operating Temperature	Operating temperature of NO2 sensor shall be 0°C to 60°C.	
8.	Operating Pressure	Operating pressure of NO2 sensor shall be $\pm 10\%$.	

6.2.5 Sulphur Dioxide (SO₂) Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	SO ₂ Sensor shall have a range of at least 0-20 PPM.	
2.	Resolution	Resolution of SO ₂ sensor shall be 0.001 PPM or better.	
3.	Lower Detectable Limit	Lower detectable limit of SO ₂ sensor shall be 0.009 PPM or better.	
4.	Precision	Precision of SO ₂ sensor shall be less than 3% of reading or better.	
5.	Linearity	Linearity of SO ₂ sensor shall be less than 1% of full scale.	
6.	Response Time	Response time of SO ₂ sensor shall be less than 60 seconds.	
7.	Operating Temperature	Operating temperature of SO ₂ sensor shall be 0°C to 60°C.	
8.	Operating Pressure	Operating pressure of SO ₂ sensor shall be ±10%.	

6.2.6 Carbon Dioxide (CO₂) Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	CO ₂ Sensor shall have a range of at least 0-5000 PPM.	
2.	Resolution	Resolution of CO ₂ sensor shall be 1 PPM or better.	
3.	Lower Detectable Limit	Lower detectable limit of CO ₂ sensor shall be 10 PPM or better.	
4.	Precision	Precision of CO ₂ sensor shall be less than 3% of reading or better.	
5.	Linearity	Linearity of CO ₂ sensor shall be less than 2% of full scale.	
6.	Response Time	Response time of CO ₂ sensor shall be less than 60 seconds.	
7.	Operating Temperature	Operating temperature of CO ₂ sensor shall be 0°C to 60°C.	
8.	Operating Pressure	Operating pressure of CO ₂ sensor shall be ±10%.	

6.2.7 PM₁₀ Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	Range of PM ₁₀ shall be 0 to 450 micro gms / cu.m or better.	
2.	Lower Detectable Limit	Lower detectable limit of particulate profile sensor shall be less than 1 µg/m ³ .	
3.	Accuracy	Accuracy of particulate profile sensor shall be <± (5 µg/m ³ + 15% of reading).	
4.	Flow Rate	Flow rate shall be 1.0 LPM or better.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Operating Temperature	Operating temperature of the sensor shall be 0°C to 60°C.	
6.	Operating Pressure	Operating pressure of the sensor shall be $\pm 10\%$.	

6.2.8 PM2.5 Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Range	Range of PM2.5 shall be 0 to 230 micro gm / cu.m or better	
2.	Lower Detectable Limit	Lower detectable limit of particulate profile sensor shall be less than 1 $\mu\text{g}/\text{m}^3$.	
3.	Accuracy	Accuracy of particulate profile sensor shall be $< \pm (5 \mu\text{g}/\text{m}^3 + 15\% \text{ of reading})$.	
4.	Flow Rate	Flow rate shall be 1.0 LPM or better.	
5.	Operating Temperature	Operating temperature of the sensor shall be 0°C to 60°C.	
6.	Operating Pressure	Operating pressure of the sensor shall be $\pm 10\%$.	

6.2.9 Noise Sensor

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Noise sensor shall detect the intensity of the ambient sound in a particular area.	
2.	General	Nosie Sensors shall be installed for the outdoor applications.	
3.	Range	Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA.	

6.2.10 Air Quality Parameter Display

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Size	LED Display - Minimum 600x1000 mm to show complete parking availability information	
2.	Pitch	13 mm (H) X 13 mm (V)	
3.	Colour	Amber coloured LED - Day Light Readable	
4.	Minimum & maximum viewing distance and angle of viewing	Viewing distance 20-100 meters Angle of viewing - Minimum 60°V – 110°H	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Vibration standard AIS 12/AIS:062 -10g	2g	
6.	Communication protocol	GPRS, RF, RS485 etc. as per site requirement	
7.	Controller and antenna	Inbuilt	
8.	Environmental specifications	(a) Temperature: 0 to +55 deg C (b) Thermal cycling: 5 Deg C/mt (c) Humidity: 5% to 95% RH (d) Sealing: IP 65 (Front), IP 54 (Rear)	
9.	Minimum life	50,000 Hrs	
10.	Data format	Bitmap or Unicode	
11.	Power supply	90 V to 250 V AC; 50 VA	
12.	Update of Information	Real-time (configurable refresh rate)	
13.	Display Format	Multimedia content, text in Hindi, English and Gurmukhi/ with presentation in tables, fixed and scrolling text	
14.	Structure	Light weight structure with toughened glass fixed with UV resistant adhesive in front	
15.	Compliance	IS /IEC 60947-1:2004 in conjunction with IS/IEC 60529:2001	

6.3 Waste Water Sensor

6.3.1 Multi-Parameter Smart Controller (Micro-Station) for COD, BOD, TSS, pH, Dissolved Oxygen, NH4-N, Temperature, Oil and Grease parameters

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> • Micro-Station/Controller shall have the latest features of highly advanced Multi Parameter Controller having capability of handling at least 4 Sensors in a single controller configuration and more as and when required with Sensor ID recognition and high EMC interference immunity • It shall be supplied with Modular Plug and Play system in which sensor can be added/changed at any time and at any location • It shall be supplied with Sensor ID recognition feature with high interference immunity. • The device shall be with easy Panel Mounting with required accessories. • Controller shall have the capability to be operated as Controller (having programmability feature) or just a terminal (that can display the data without any way to make changes). 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		The Micro-Station shall be able to power all the sensors and terminals or accessories attached to it without having to need any additional power sources in the system for increased protection against lightening and possible electromagnetic interference	
2.	Display	The device shall be supplied with large graphic display with backlight. Display shall be with improved reading precision through special backlit graphic display	
3.	Electrical	Input voltage: 220 VAC and 50 Hz Output: Galvanically separated current outputs (0/4-20 mA) that can be assigned arbitrarily, RJ45 Ethernet availability, USB-interface for data transfer, upgrading firmware etc. The system should start automatically after the power is reset to the system (in case of power failure). The system should have Service mode for cleaning/calibration/maintenance activities. The controller shall store the sensor configurations and calibrations The controller shall have Logbook to record the data The supplier shall provide the firmware update free of cost as and when they are available for the life time of the system	
4.	Interfaces	External interfacing with IEG (Intelligent Edge Gateway) using Modbus interfaces.	
5.	Measuring Parameters	COD, BOD, TOC, TSS, pH, Temperature, Dissolved Oxygen, Conductivity, NH4-N, Oil & Grease etc.	
6.	Operating Temperature	Ambient Operating temperature: -20 °C to 55 °C, Storage temperature: -10 °C ... 60 °C	
7.	Process Connection	1" PVC type process Connection	
8.	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable	
9.	Protection	<ul style="list-style-type: none"> Electromagnetic Compatibility: EN 61326, Class B; FCC Class A, EMC for indispensable operation Integrated Lightening protection, Protection Rating IP 66	
10.	Calibration	Timely Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period.	
11.	Certification	CE/UL/EN/BIS	
12.	Cables	Necessary cables for power, communication and data	
13.	Accessories and Laying	Bidder shall provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		complete and integrated system without any extra cost to tendering authority.	
14.	Display	The device shall be supplied with large graphic display with backlight. Display shall be with improved reading precision through special backlit graphic display	

6.3.2 Sensor Probe for BOD/COD/TSS Analyzer

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> The probe shall be a Multi parameter Probe. It shall be continuously Effluent Monitoring of BOD, COD, TOC, TSS with UV-Vis Full Spectrum Technology. It shall be ideally for Waste Water measurements in Open Channel with direct In-Situ measurement along with floating type arrangement using SS chain. It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation The device shall be with easy Mounting without Clogging The Sensor should provide compensation of interferences by evaluation of the whole measured spectrum. 	
2.	Measuring Principle	It shall have the UV-Vis Spectrometry principle for measurement over the total Range (190 - 720 nm)	
3.	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable	
4.	Cleaning	The probe shall be supplied with Integrated cleaning system	
5.	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration. Timely Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period	
6.	Measuring Parameters	BOD, COD, TOC, TSS	
7.	Accuracy	±2%	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
8.	Operating Temperature	0° C to 50° C	
9.	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface	
10.	Protection	The Probe shall support the IP68 protection standard	
11.	Protection	The device shall have the conformity to EMC and Safety with EN 61326-1, EN 61326-2-3 and EN 61010-1 standards	
12.	Protection	The sensor should be completely reagent free for operation.	
13.	MOC	The MOC must be Titanium Material or equivalent to sustain the sensor in highly corrosive wastewater environment.	
14.	Light Source	Xenon Flash Lamp	
15.	Measuring Range	COD: 0 - 20000 mg/l BOD: 0 - 8000 mg/l TOC: 0 - 20000 mg/l TSS: 0 - 4500 mg/l However, SI shall conduct the site survey and range of the probes shall be according to the site survey / Lab Report.	
16.	Accessories and laying	Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.	

6.3.3 Sensor Probe for Dissolved Oxygen (Dissolved Oxygen)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> The probe shall be a Multi-parameter Probe It shall be used ideally for Open Canal (Floating Type) It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation Long term stable and maintenance free operation 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	Resolution	0.01 mg/l O ₂	
3.	Measuring Principle	Mounting and Measurement shall be directly in the media or in a flow cell (Monitoring Station)	
4.	Cleaning	The probe shall have the optical/ fluorescence measurement principle	
5.		The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable	
6.	Calibration	Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC	
7.	Measuring Parameters	Long term stable and maintenance free operation	
8.	Accuracy	The probe shall be factory pre-calibrated and with local multi-point calibration	
9.	Operating Temperature	Dissolved Oxygen	
10.	Interface to Scanner	±1%	
11.	Protection	0° C to 60° C The probe shall be interface with Scanning terminal using RS 485 interface	

6.3.4 Sensor Probe for Nitrate (NO₃-N) and Ammonical Nitrogen (NH₄-N)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> It shall be ideally for Waste Water Treatment Process It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation Ion Selective Electrodes Refurbishment for easy maintenance Mounting and Measurement shall be directly in the media or in a flow cell (Monitoring Station) 	
2.	Measuring Principle	It shall have the Ion selective electrodes without potassium compensation for measurement	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable The probe shall be supplied with Integrated cleaning system	
4.	Calibration	The probe shall be Factory calibrated with optional In-Situ calibration for improved accuracy. Timely Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period	
5.	Measuring Parameters	NH4-N, NO3-N	
6.	Accuracy	±3%	
7.	Operating Temperature	0° C to 60° C	
8.	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface	
9.	Protection	The Probe shall support the IP68 protection standard Conformity to EMC with EN 50081-1, EN 50082-1, EN 60555-2, EN 60555-3 & to safety with EN 61010-1 standards	
10.	Cable	The Sensor cable supplied along with the sensor shall be 15 Meters and of Sea Water version so that it's not affected by acids and presence of highly corrosive media in sample.	
11.	Measuring Range	0.1 ...1000 mg/l NO3-N 0.1 ...1000 mg/l NH4-N However, SI shall conduct the site survey and range of the probes shall be according to the site survey / Lab report.	

6.3.5 Sensor Probe for pH and Temperature

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> The probe shall be a Multi-parameter Probe It shall be ideally for Waste Water monitoring Process in an Open Channel (Floating Type) It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment 	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<p>for long term stable and maintenance free operation</p> <ul style="list-style-type: none"> • Long term stable and maintenance free operation • Integrated temperature measurement and compensation shall be provided in the pH sensor. <p>The pH sensor should have Galvanically separated input. Temperature Sensor shall be integrated in the pH sensor.</p>	
2.	Cleaning	The pH combination electrodes shall be required very little maintenance and there should be no electrolyte replacement (Reagent Free).	
3.	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable	
4.	Calibration	Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC	
5.	Measuring Parameters	Probe shall use the Electro Chemical measuring principles to measure the pH and Temperature.	
6.	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration	
7.	Measuring Range	Measuring Range: pH: 0.00- 14.00 at least considering the waste water environment Measuring Range Temperature: -5 to 60° C	
8.	Operating Temperature	Temp Compensation: -5 to 50° C	
9.	Accuracy	±1%	
10.	Interface	The probe shall be interface with Scanning terminal using RS 485 interface	
11.	Sensor Cable	The Sensor cable supplied along with the sensor shall be 15 Meters and of Sea Water version so that it's not affected by acids and presence of highly corrosive media in sample.	
12.	Measuring Range	Measuring Range: pH: 0.00- 14.00 units at least considering the wastewater environment Temperature Measuring: -5 to 60 Deg C	
13.	Accessories and Laying	Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.	

6.3.6 Sensor Probe for Oil & Grease Analyser (Open Channel, Floating Type)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> The probe shall be used to measure Oil and Grease in waste water using UV fluorescence technology. It shall be ideally for Waste Water Treatment Process It shall have Long term stable and maintenance free operation 	
2.	Housing	The Probe shall be supplied with stainless steel, Titanium housing material	
3.	Mounting	The probe shall be vertically mounted	
4.	Measuring Principle	The probe shall have the UV fluorescence (254 - 360 nm) measurement principle	
5.	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable The probe shall be supplied with Integrated cleaning system	
6.	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration. Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC	
7.	Measuring Parameters	Oil & Grease	
8.	Limit of Detection	1 µg/L	
9.	Operating Temperature	0° C to 60° C	
10.	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface	
11.	Protection	The Probe shall support the IP68 protection standard Conformity to EMC with EN 50130-4, 61000 - 6-1standards	
12.	Accessories and Laying	<ul style="list-style-type: none"> Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority. 	

6.3.7 IEG with integrated 3G/4G communication capabilities with Cable and other Accessories

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> Industrial grade IEG with Analog input channels shall be supplied for integrating various quality Analysers / controllers to monitor the waste water quality parameters. The device shall have interfaces to integrate quality analysers/controllers using Modbus RTU interfaces for upstream communication. It shall have be hot plug and play device with minimum configuration. It shall have inbuilt real-time clock with synchronization from GSM network The device shall have easy Extension and Adaptation facility 	
2.	Environmental	<ul style="list-style-type: none"> The supplied unit shall perform the vibration tests producing certificates from National Standard Laboratories EMI / EMC certified The device shall be suitable for hazardous environment and shall be IP 67 standard of protection 	
3.	Mechanical	<ul style="list-style-type: none"> Din Rail mounted with Input module The device shall be supplied with fixtures for Pipe mounting / wall mounting / Panel mounting possibilities. 	
4.	Electrical	<ul style="list-style-type: none"> Power Supply: 220V AC IP66 to EN 60529/09.2000 Complies with NEMA 4. Accuracy: 0.1% Span: > 0 to 20 mA Resolution of current inputs: < 5 μA Nominal Input Current: Max. 8 mA Signal Characteristic: Linear Internal Resistance: Non-Linear The supplied unit shall have over voltage and Lightning protection feature Easy remote configuration and software update facilities Inbuilt plug-in I/O support Electrical Safety: IEC 61010-1, Class I equipment 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> Low voltage: overvoltage category II protection Memory: 16 MB flash, 2 MB RAM 	
5.	Communication	<ul style="list-style-type: none"> Communication shall be over Modbus / Ethernet IP/ Any Open IoT protocols such that it shall be able to send data to centralized application server (OWQMS) over GSM / GPRS network using 3G/4G enabled inbuilt modems. Interfaces: RS485 half-duplex, 8kV air discharge protection, 4kV,ESD Protection Contact The device shall be integrated with Central applications for waste water quality data analysis 	

6.3.8 Field Enclosure / Panels for Waste water Quality Monitoring Stations / Controllers, IEG

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Built	The Outdoor Utility Cabinet shall be constructed with a front sheet steel door with Locking system to ensure the security of the cabinet. Side and Wall Panels shall be with fixing bolts internal to the cabinet. The Cabinet should have the required frames to mount the required components like Field equipment such as IEG / DCU / Gateways / MCT / Analysers, Power supply Equipment, Networking Equipment, LIU, battery, etc.	
2.	Utility & IP rating	Should be designed for 24 X7 X 365 Outdoor Applications; The Utility Cabinet shall be IP67 or better rated with built-in air-cooling system. Field Enclosure design should ensure to keep the operating temperature / ambient temperature within suitable operating range 20° C to 55° C for equipment's and should also avoid condensation, corrosion, intentional water splash and dust intake.	
3.	Size	The cabinet shall be provided of size suitable for the mounting of the associated network devices, power, UPS and battery components securely and safely within the cabinet.	
4.	Power Slot	PDU type should be as per actual requirement as per Indian standards.	
5.	Cable Management	Proper cable management should be provided.	

6.4 Network Backbone

6.4.1 Industrial grade Field Layer-2 FE 8 port POE Switch

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Features	<ul style="list-style-type: none"> The switch should provide minimum 8 X 10/100/1000 BaseT access ports & 4xGE combo uplink ports. Switch should have minimum 120W PoE power available or extra power injector should be provided in the junction box The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate Should support minimum 12 Gbps or more, full duplex wire rate switching throughput Switch must support Ethernet CFM / CFM (IEEE 802.1ag), Performance monitoring (ITU T Y.1731) and Unit-Directional Link Detection (UDLD) from day 1 	
2.	Layer 2 Features	<ul style="list-style-type: none"> 802. 1Q VLAN on all ports 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. 	
3.	Layer 3 Features	Static, Inter-VLAN routing must be enabled from day one	
4.	Quality of Service (QoS)	<ul style="list-style-type: none"> Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port 	
		<ul style="list-style-type: none"> The switch should provide traffic shaping and rate limiting features for specified Host, network, Applications etc. 	
5.	Security Features	<ul style="list-style-type: none"> The switch should support ACLs, 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. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
6.	Management Features	<ul style="list-style-type: none"> 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, FTP/TFTP 	
7.	Mechanical Conditions:	<ul style="list-style-type: none"> Temperature: -5 to +70°C Operating relative humidity: 5% to 95% no condensing Protection Class -minimum IP 30, NEMA-TS2 	
8.	Certifications	<ul style="list-style-type: none"> Switch should be EN 55022 certified. The switch should support NTP EMC interface immunity: Switch should be EN 61000-4-2 Electro Static Discharge, EN 61000-4-5 Surge, EN 61000-4-8 Power Frequency Magnetic Field 	
9.	POE	Switch shall support persistent PoE power and shall allow the PD's to retain power in case the switch undergoes a reboot helping PoE Devices with built in storage to continue operation and sync up on network availability.	
10.	POE	Switch shall support per-Port PoE configuration	

6.4.2 Industrial grade Field Layer-2 FE 16 port POE Switch

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Genera	The switch should provide Minimum 16 port or 2 X 8 Ports of 10/100/1000 Mbps GE ports and 4 GE SFP uplinks Ports. Should be proposed with ruggedized transceivers as per solution. The switch shall be DC powered. Should support minimum 20 Gbps or more, full duplex wire rate switching throughput	
2.	Layer 2	802.1Q VLAN on all ports with support for minimum 400 active VLANs	
3.	PoE	Switch should have minimum 120W PoE power available or extra power injector should be provided in the junction box	
4.	Layer 2	Spanning Tree Protocol as per IEEE 802.1d, 802.1s and 802.1w	
5.	Layer 2	Should support Improved resiliency with the support of Resilient Ethernet Protocol (REP) or equivalent ITU-T standard for ring topology which should provide 50ms ring convergence	
6.	Layer 3	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
7.	General	Switch should support non-blocking throughput and IPv4 & IPv6 routes	
8.	L2	Switch should support classification and scheduling as per IEEE 802.1P	
9.	QoS	Switch should support strict priority queuing or Policing or equivalent to guarantee that the highest-priority packets are serviced ahead of all other traffic.	
10.	Certification	RoHS Compliant, IEEE 802.3af, 802.3at, NTP	
11.	Environmental	Operating Temperature 0 C to +70C with fan less design	
12.	Environmental	Relative Humidity of 5% or 95% Non-condensing	
13.	Certification	Switch should be EN 61000-4-2 Electro Static Discharge, EN 61000-4-5 Surge, EN 61000-4-8 Power Frequency Magnetic Field, EN61000-4-6 for Conducted susceptibility	
14.	Certification	Must support FCC 47 CFR Part 15 Class A/ FCC Part 15B, Class A	
15.	Standard	EN 55022	
16.	Standard	Protection Class -minimum IP 30, NEMA-TS2	
17.	Power	Switch shall support persistent PoE power and shall allow the PD's to retain power in case the switch undergoes a reboot helping PoE Devices with built in storage to continue operation and sync up on network availability.	
18.	PoE	The switch shall support per-Port PoE configuration	

6.4.3 Junction Box 1 KW (Outdoor Utility Cabinet)

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Mechanical Structure	<ul style="list-style-type: none"> Out Door Cabinet with Pole/Ground/Wall Mount provision with all civil work required as per design approved by ASCL & AMC Material – Galvanized Iron (GI) Sheet Thickness – Enclosure structure using 1.6 mm Foot plinth panel sheet minimum 3mm 	
2.	Ingress Protection	IP 55 Rated	
3.	Colour	Colour - Grey / Relevant	
4.	Coating thickness	Powder coating thickness between 70 to 120 micron Finish	
5.	Cables	Cable management must be ensuring proper path for AC supply	
6.	Cable Entry	Cable entry on side bottom/Side wall through cable glands of PVC material to ensure rain water protection.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
7.	Cooling	Forced air cooling to maintain equipment at optimal temperature	
8.	Filter	Removable and washable type pleated filters with aluminium wire mesh protection on both sides.	
9.	Earthing	Diagonal opposite bolt on bottom frames and individual door for body earthing. Internally door shall be grounded with the main frame.	
10.	Door Open Switch	Required for alarm extension, fan working and lighting. In case of any door open, alarm shall be generated.	
11.	Free Space	Free Space: minimum 4U	
12.	Input Voltage Range	180 - 300 V	
13.	Frequency (default: sync range)	50 HZ	
14.	Protection	Inbuilt Short Circuit, Over/ Under Voltage	
15.	Surge Protection	Class C type (IEC 61643-1, UL 94-0)	
16.	Power Factor / THD	> 0.9 at 50% load or more / < 5%	
17.	System Total (AC+DC) Usable Capacity	1 KW	
18.	Minimum DC Capacity	As per site requirement	
19.	Minimum AC Capacity	As per site requirement	
20.	Nominal System Output Voltage	220V AC/ Sine Wave	
21.	Frequency	50Hz +- 5%	
22.	Overload Protection	Yes	
23.	THD	<5%	
24.	Protection	Short Circuit, Over Temperature	
25.	Crest Factor	3	
26.	Efficiency	89% @ full load	
27.	Output Ports	As per site requirement	
28.	Controls and Monitoring	Embedded Controller with LCD display	
29.	User interface	<ul style="list-style-type: none"> • LEDs for local visual alarming (Major, Minor, Power ON) • Ethernet for remote or local monitoring and control via Web browser. • SNMP V2 & V.3.0 protocol 	
30.	Operating temperature	0 to +65 °C	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
31.	Battery Technology	Support both VRLA/SMF and Lithium Iron Phosphate.	
32.	Remote Management	Monitoring battery alarms, energy consumption, On/Off of connected loads and parameters.	
33.	Battery Backup	2 Hrs	

6.4.4 Junction Box 2 KW (Outdoor Utility Cabinet)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Mechanical Structure	Out Door Cabinet with Pole/Ground/Wall Mount provision with all civil work required as per design approved by ASCL & AMC Material – Galvanized Iron (GI) Sheet Thickness – Enclosure structure using 1.6 mm Foot plinth panel sheet minimum 3mm	
2.	Ingress Protection	IP 55 Rated	
3.	Colour	Colour - Grey / Relevant	
4.	Coating thickness	Powder coating thickness between 70 to 120 micron Finish	
5.	Cables	Cable management must be ensuring proper path for AC supply	
6.	Cable Entry	Cable entry on side bottom/Side wall through cable glands of PVC material to ensure rain water protection.	
7.	Cooling	Forced air cooling to maintain approx. T < 10 Degree	
8.	Filter	Removable and washable type pleated filters with aluminium wire mesh protection on both sides.	
9.	Earthing	Diagonal opposite bolt on bottom frames and individual door for body earthing. Internally door shall be grounded with the main frame.	
10.	Door Open Switch	Required for alarm extension, fan working and lighting. In case of any door open, alarm shall be generated.	
11.	Free Space	Free Space: minimum 8U	
12.	Input Voltage Range	230 - 300 V	
13.	Frequency (default: sync range)	50 HZ	
14.	Protection	Inbuilt Short Circuit, Over/ Under Voltage	
15.	Surge Protection	Class C type (IEC 61643-1, UL 94-0)	
16.	Power Factor / THD	> 0.9 at 50% load or more / < 5%	
17.	System Usable Capacity	2 KW	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
18.	Maximum DC Capacity	As per requirement	
19.	Maximum AC Capacity	As per requirement	
20.	Nominal System output Voltage	220V AC/ Sine Wave	
21.	Frequency	50Hz +- 5%	
22.	Overload Protection	Yes	
23.	THD	<5%	
24.	Protection	Short Circuit, Over Temperature	
25.	Crest Factor	3	
26.	Efficiency	89% @ full load	
27.	Output Ports	Miscellaneous X 2 (3 Amp)	
28.	Controls and Monitoring	Embedded Controller with LCD display	
29.	User interface	<ul style="list-style-type: none"> LEDs for local visual alarming (Major, Minor, Power ON) Ethernet for remote or local monitoring and control via Web browser. SNMP V2 & V.3.0 protocol 	
30.	Operating temperature	0 to +65 °C	
31.	Battery Technology	Support both VRLA/SMF and Lithium Iron Phosphate.	
32.	Remote Management	Monitoring battery alarms, energy consumption, On/Off of connected loads and parameters.	
33.	Battery Backup	2 Hrs	

6.5 Variable Message Display (VMD) Board

6.5.1 VMD board including VMD controller and Cabinet IP66 Compliant

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Technology	Full Colour (cluster of red, green and blue diodes) as per IRC/EN 12966 standard	
2.	Luminance Class	L3 as per IRC/EN 12966 standards	
3.	Dimming Control	<ul style="list-style-type: none"> Automatic Luminance control and auto dimming capability to adjust as per ambient light level (sensor based automatic control). It shall also be capable of being configurable and controlled by VMS operator from the Traffic Monitoring Center. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> 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. 	
4.	Contrast Ratio	R3 as per IRC/EN 12966 standard or >30 perpendicular to the bold face and >10 at an angle of 70 degrees to the perpendicular	
5.	Beam Width	B3 as per IRC/EN12966 standards.	
6.	Pixel Pitch	20mm or better	
7.	Picture Display	i. Character height up-to 400mm as per IRC/EN 12966 standards ii. Number of lines & characters adjustable iii. Synchronized Dot to Dot display. iv. Capable of displaying real-time message generated by ICCC v. Special frontal design to avoid reflection. vi. Display shall be UV resistant	
8.	Viewing Angle	Horizontal -110 degree – 140 degree Vertical -50 degree – 70 degree (Viewing angle shall ensure message readability for motorists in all lanes of the approach road)	
9.	Self-Test	i. VMS shall have self-test diagnostic feature to test for correct operation. ii. Display driver boards shall test the status of all display cells in the sign even when diodes are not illuminated	
10.	Refresh Rate	Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.	
11.	White Balance Brightness (cd/m2)	> 6500 – 8000 (Adjustable)	
12.	Multiple Data Communication interface/Port	RJ45 Ethernet, RS232, RS 485	
13.	Communication (connectivity)	GSM/GPRS/3G/4G or any suitable for the system to display the information on VMS on real-time basis.	
14.	Ambient Operating Temperature	The system should be capable of working in ambient temperature range of -5 degree C to 55 degree C.	
15.	Humidity (RH).	Operating ambient humidity: 10% - 95% Rh or better	
16.	Protection against Pollution/dust/water	Complete VMS should be of IP 65 protection level. As per EN60529 or equivalent Standard.	
17.	Power	i. 170-250V AC (more than 95% power factor) or DC as per equipment requirement. ii. Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated. iii. The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
18.	Power Back-up & its enclosure	Inverter/UPS for 2 hours power back-up with auto switching facility. The enclosure of Inverter/UPS and battery should be pole mountable with IP 65 protected housing and lockable	

6.5.2 Mounting structure for VMD

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Overhead Gantry includes providing and fixing of retro-reflectorized Informatory /Direction sign Boards made of 4mm thick Aluminium Composite Material Sheet, face to be fully laminated with orientation free Micro Prismatic Grade Sheeting as defined in IRC: 67-2012 Class C Type IX or XI having approved messages e.g. letter, numerals, symbols /legend/arrow etc. in Hindi and /or English, to be cut out from durable transparent Overlay Electrocutable film or digitally printed using Traffic jet or similar eco solvent printer, subsequently over laminated by sheeting manufacturer's OEM protective transparent overlay to achieve minimum 10 years outdoor life	
2.	General	There will be messages on both side of the board	
3.	General	The width of Overhead structure will be variable from of 14 m to 40 m depending upon width of carriageway. There must be clear distance of at least 2.5 m from edge of road at both shoulders	
4.	General	Middle sign post (If installed) may be installed at Median of the road. There should be aluminium backing based hazard marker pasted on both visible ends of RCC pedestal to enhance visibility at night time	
5.	General	Minimum lateral clearance of sign post from crown level of road should be 6 m. Minimum height of way finder panel must be 3 m.	

6.6 Sewerage Treatment Plant Integration

6.6.1 Ethernet to 3G/4G Router with high power antenna of minimum 12 dBi

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The Router shall be internet 4G LTE mobile broadband to Ethernet Router with desired security suite, supporting VPN Server and client configurations. Functionalities into a single box.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	General	Router shall have High performance antenna (of minimum 12 dBi) for optimal 3G / 4G LTE services.	
3.	General	The device shall support fall back to 3G when 4G/LTE is not available	
4.	General	Router shall have 4 Fast Ethernet ports (10/100 – Mbps Managed Switch) to connect wired devices to the network	
5.	General	The device shall have Ethernet WAN port for wired broadband service.	
6.	General	The device shall support feature like deploying in many different environments where space, heat dissipation, and low power consumption are critical factors.	
7.	General	The router shall support hi-speed IP Security (IPsec); 3DES and AES encryption offer data privacy over the Internet with Intrusion prevention which shall enforces security policies in a larger enterprise or service provider network.	
8.	General	Router shall have the Scan Safe web security and filtering solution that requires no additional hardware or client software.	
9.	General	It shall do the Content filtering offers category-based URL classification and blocking, thus providing increased productivity and better use of company resources.	
10.	General	Router shall be maintaining the assigned IP addresses to the home network in private or public networks.	

6.7 Data Centre

6.7.1 Surveillance Storage (1300 TB NL SAS Drives Usable Capacity)

Bidder may propose Storage Optimized Server with Virtualization Software or External SAN to store Video.

Option 1: Storage Optimized Server with Virtualization Software

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Storage Optimized Server with Virtualization Software	Proposed make of Storage Optimized Server with Virtualization Software should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Storage Optimized Servers should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the Servers and Servers to the Video Recording Server Cluster.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	Processors	Controller/node shall have a minimum of 14 cores or more, 2.4 GHz with dual sockets. Each node shall be provided with virtualization software and should not host more than 4 VM's.	
3.	Memory	Controller/node should provide 128 GB or more memory scalable to 256 GB	
4.	Drives	Capacity: The storage must support SAS, SSD and NL SAS disks simultaneously. For balanced performance, rebuild time & capacity, the storage should be provisioned with minimum 1300 TB of Usable capacity (RAID 6, 8D+2P configuration) with maximum 8TB NL-SAS drives. Minimum two spare drives of proposed disk type to be provided for every Controller. 2 Drives of proposed capacity to be configured & kept at the site as cold spares.	
5.	Upgradability	Server/Controller nodes should be upgradeable without having to change the entire chassis	
6.	Storage	In case of failure, individual drives can be replaced without impacting any other drives	
7.	Cache	Should be provided with minimum on-board Flash Backed Write Cache of up to 2 GB or higher	
8.	Network	Provide Minimum 2X10Gbps per controller/server node.	
9.	Replication to Cloud	The solution should include a host based replication license for replicating the VM's to cloud. It should include an end to end encryption without impacting the data reduction ratios of built-in compression and WAN acceleration	
10.	Redundancy	Should be provided with redundant power supplies and fans.	
11.	Performance	Storage Solution should be sized to accept 100% writes from minimum 1400 Number of IP cameras @3Mb/s. On top of performance required to write from cameras the storage Solution should be sized to accept 100% headroom to accommodate future growth. (Compute Power)	
12.	Rack	System must be modular & Rack mountable.	
13.	Others/Misc.	<ul style="list-style-type: none"> Storage Optimised Server must be supplied with all necessary software for carrying out all management (configuration, diagnostics etc.) activities on the storage. All required cables must be supplied. Necessary Mounting Kit to install the Storage server in a 42U rack must be supplied. 	
14.	Scalability	The capacity of the proposed configuration should be 100% scalable with the proposed disk configuration. No additional software/feature license or controller(s) should be required for further 100% capacity	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		expansion. It should support SSD, NL-SAS and enterprise SAS Drives in the same enclosure for future expansions.	
15.	Software Licenses	For investment protection, all licensed features of the array must be enabled as perpetual license for full scalable capacity of the proposed storage array.	
16.	Storage Resource Management Software	All the necessary software (GUI Based) to configure and manage the storage capacity, RAID configuration, Snapshots, clones, Thin Provisioning, Role based Access Control (RBAC) with audit Logs, Remote replication, VAAI, ODX etc. are to be provided.	
17.	Integration	The proposed storage solution must integrate with the Unified All Flash Storage through the VMS software for cloud backup & replication.	

Option 2: SAN Storage

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	SAN Storage	Proposed make of SAN storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed SAN should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & controllers to the FC SAN & IP SAN fabric with all the controllers managed from a One single GUI based management Interface. All requirements specified are minimum.	
2.	SAN Controllers	Hot-pluggable Active-Active Storage Controllers	
3.	Backend Connectivity	To eliminate single point of failure from the controller to the backend storage, each storage controller must have redundant 12Gb/s or higher backend connectivity i.e. 2 X 12Gb/s SAS ports or better per controller.	
4.	Frontend Host Interface	Minimum 4 Number of FC SAN Host Ports @16 Gbps or higher and Minimum 2 Number of IP SAN Host Ports @10Gbps or higher per controller.	
5.	Drives	Capacity: The storage must support SAS, SSD and NL SAS disks simultaneously. For balanced performance, rebuild time & capacity, the storage should be provisioned with minimum 1300 TB of Usable capacity (In RAID 6, 8D+2P configuration) with maximum 8TB NL-SAS drives. Minimum two spare drives of proposed disk type to be provided for every Controller. 2 Drives of proposed capacity to be configured & kept at the site as cold spares.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
6.	Cache	Cache: minimum 96GB DRAM cache across dual controller. Battery/Flash based cache protection for minimum 72 hours should be provided. Cache specified is minimum. Bidders must offer more cache if required for the proposed solution.	
7.	RAID levels support	Should support various RAID levels (5,6,10) or equivalent.	
8.	OS support	Support for industry-leading & OEM supported Operating System platforms of CentOS, Linux, IBM AIX, Microsoft Windows Server, Novell SUSE Linux Enterprise Server, Oracle Enterprise Linux, Oracle Solaris, Red Hat Enterprise Linux, Ubuntu Linux & VMware ESX. If license is required for multipathing/failover drivers from the storage OEM, unlimited host license to be provided.	
9.	Rack	Storage Array must be modular & Rack mountable.	
10.	Scalability	The capacity of the proposed configuration should be 100% scalable with the proposed disk configuration. No additional software/feature license or controller(s) should be required for further 100% capacity expansion. It should support SSD, NL-SAS and enterprise SAS Drives in the same enclosure for future expansions.	
11.	Enterprise SAN features	Enterprise SAN Storage should support hot plug of controllers, hard disk drives, power supplies & fans. Since the video streams will be on this storage, the proposed storage must have online storage OS & drive firmware update/upgrade capability.	
12.	Fans and Power supplies	Redundant power supply and cooling fans.	
13.	Software Licenses	For investment protection, all licensed features of the array must be enabled as perpetual license for full scalable capacity of the proposed storage array.	
14.	Storage Resource Management Software	All the necessary software (GUI Based) to configure and manage the storage capacity, RAID configuration, Snapshots, clones, Thin Provisioning, Role based Access Control (RBAC) with audit Logs, Remote replication, VAAI, ODX etc. are to be provided.	
15.	Others/Misc.	<ul style="list-style-type: none"> Storage must be supplied with all necessary software for carrying out all management (configuration, diagnostics etc.) activities on the storage. All required cables must be supplied. Necessary Mounting Kit to install the SAN storage in a 42U rack must be supplied. 	
16.	Integration	The proposed storage solution must integrate with the Unified All Flash Storage through the VMS software for cloud backup & replication.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
17.	Performance	Storage Solution should be sized to accept 100% writes from minimum 1400 Number of IP cameras @3Mb/s. On top of performance required to write from cameras the storage Solution should be sized to accept 100% headroom to accommodate future growth.	

6.7.2 Unified storage with SAN Switch (75TB for Video and Application Data)

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Unified Storage	Proposed make of Unified All Flash storage system should be from reputed brands of Storage System's OEM. For investment rationalization, the proposed Unified All Flash storage system should be modular & scalable in nature wherein the Storage can be scaled by adding capacity to the controllers & controllers to the FC SAN & IP SAN fabric as well IP NAS network with all the proposed controllers managed from a One single GUI based management Interface. All requirements specified are minimum.	
2.	Solution Type	Bidder is expected to provide Unified Storage solution should have block and file access with host connectivity for FC, iSCSI, CIFS and NFS. Storage should have the capability to scale up and scale-out. The unified storage solution must be dedicated appliance with specifically optimized OS to provide both SAN and NAS functionalities. Proposed storage system must have minimum 2 Unified controllers. The all proposed All Flash storage system should be categorized as All Flash Array/Solid State Array by the OEM & optimised for Solid State Drives (SSDs).	
3.	Storage Size	Storage should be supplied with 75TB of usable space with maximum 8TB, 12Gbps SSD Drives. Usable space is space without space efficiencies/gains from Dedupe, Compression etc.	
4.	Hardware Platform	Rack mounted form-factor Modular design to support disk drives expansion 4 X 12Gbps SAS ports for Backend disk connectivity. The proposed storage must scale up to minimum of 1.5 times number of SSD drives proposed. Hot spares should be configured as per OEM best practices & 1 cold spare disk should be offered onsite with the storage.	
5.	Controllers	Unified Storage controller nodes must be configured in Dual-Active configuration. Storage controller must have minimum 32GB on-board Protected cache per controller. The controllers /Storage nodes should be upgradable seamlessly, without any disruptions/downtime to production workflow for	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		performance, capacity enhancement and software/firmware upgrade. In case bidder is offering different controllers for SAN & NAS features, every controller in the solution must have same cache & ports available to hosts.	
6.	Front end host Ports	Minimum 4 X 16Gbps FC, 4 X 10Gbps IP Ports	
7.	Operating System and Virtualization Support	The storage solution should support all latest operating system and cluster environments The unified storage solution should support virtual infrastructure (like VMware / Hyper-V etc). Should have capabilities for booting VMs from the SAN. Should be supplied with virtualization aware APIs for provisioning and managing the storage array from the virtual infrastructure.	
8.	Unified Protocol Support	Storage should support protocol – FC, iSCSI, NFSv3, CIFS and SMB	
9.	Management Protocol Support	SNMP and NTP Synchronization	
10.	RAID support	Should support various RAID levels (5,6,10) or equivalent	
11.	Multi-pathing and SAN Security	The multi-pathing software should provide multi-pathing from all leading OEM's. The Storage should provide provision LUN Masking and SAN Security	
12.	Redundancy and High Availability	The Storage System should be able to protect the data against single point of failure with respect to controller, disks, cache, connectivity interfaces, fans and power supplies. Storage should support non-disruptive online microcode upgrades & support load balancing and failover without any limitation on SAN and NAS provisioned capacity.	
13.	Management software	<ul style="list-style-type: none"> All the necessary software as specified in this RFP including capability to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc, single Command and GUI and Integrated Web Console for entire storage system for configuration for both file & block storage and associated functionalities including deployment, automation, provisioning, and protection and monitoring management. Solution should offer real-time performance monitoring tools giving information on CPU utilization, volume throughput, I/O rate and latency reports of at least 12 months. Should be able to create instantaneous or Point in Time Snapshot copies of volumes which can be either a full clone or incremental snapshot of the volumes. 	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
14.	Supported Software and licenses from day one for the total configured capacity and configured Protocols	Thin Provisioning, Inline Compression, Inline Deduplication, snapshot, restore snapshot, Cloning and application & VM aware backup. Storage system should support remote Asynchronous replication for Disaster Recovery with bandwidth optimization over WAN. Storage should be configured with data at rest encryption and key management.	
15.	Data Protection	The storage array must have complete cache protection using mechanism like mirroring/ de-staging/coherency for both file & block provisioned capacity. Also write data protection with battery backup for up to minimum 24 hours. The data shall not be lost in the case of power failure.	

6.7.3 SAN Switch

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Interface	The fibre switch should be quoted with minimum 48 FC ports of 16Gbps speed with all supported Licenses from day one.	
2.	Speed/Bandwidth	The switch should have support for 8/16 Gbps HBA	
3.	Switch Features	The switch should have auto sensing, Zoning, Integrated Ethernet and Serial Port for communication.	
4.	Form Factor	Switch should be rack mountable 1U size and should be supplied with mounting kit.	
5.	Power Supply	The switch should be equipped with redundant hot swap power supply and Fan and allow hot swap ability without resetting the switch, or affecting the operations of the switch	
6.	Compatibility	The switch should be backward compatible	
7.	General Features	The switch should be capable for Non-disruptive firmware /microcode upgrade and hot code activation.	
8.	General Features	The switch should be capable of End to end performance monitoring	
9.	General Features	The switch should have Support for POST & online /offline diagnostics, non-disruptive daemon restart FC ping and path info (FC trace route)	
10.	General Features	The switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems	
11.	General Features	The switch should have following Zoning and security features -	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
12.	General Feature	<ul style="list-style-type: none"> Support for hardware and software zoning and ACL Policy based security and centralized fabric management. Support for secure access. Support for FC based authentication. Support for RADIUS, SSH, SNMP Support for port binding. Support for port masking. Support for Hardware based Inter Switch linking / trunking. Support for dynamic Load balancing of links with no overhead. 	
13.	General Features	Support for web based management and should also support CLI. Switch shall support alert based on threshold value for temperature, fan status, power supply status and port status.	
14.	General Features	The switch shall support different port type such as FL port, F port, M port(mirror port), and E port ; self-discovery based on switch type (U port); optional port type control in access gateway mode F port and NPIV-Enabled N port.	
15.	General Features	All relevant licenses for all the above features and scale should be quoted along with switch	

6.7.4 Blade Servers (Web, Application, Database, Platform Solutions etc.)

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	CPU	Each blade shall have two numbers of latest Intel Xeon Scalable Processors with Min. 18 cores per processor each having Min. 2.3 GHz processor.	
2.	Motherboard	Intel chipset compatible with the offered processors.	
3.	Memory	Min. 24 DIMM slots, should be provided with 256 GB RAM using DDR4 DIMM's operating at 2666 MT/s (depending on processor model)	
4.	Memory Protection	Advanced ECC with multi-bit error protection, online mirror/spare memory	
5.	Hard disk drive with carrier	2X400 GB or Higher 3X DWPD SSD drives	
6.	Storage Controller	SAS Raid Controller with RAID 0/1	
7.	Networking features	The server should provide a minimum of 40 Gbps of bandwidth with Converged network adapter ports across two or more cards.	
8.	Interfaces	Minimum of 1X internal USB 3.0 port, 1X internal SD card slot	
9.	Bus Slots	Minimum of 2 Nos of PCIe 3.0 slots	
10.	Redundancy	The blades to be provided with port level & card level redundancy	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
11.	Operating System and Virtualization Support	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), VMware, SUSE Linux Enterprise Server (SLES)	

6.7.5 Server Rack - 42 U with necessary cabling

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design	19" 42U racks. All the racks should be mounted on the floor with castor wheels with brakes (set of 4 per rack)	
2.	Design	Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium 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.	
3.	Design	The racks should conform to EIA-310 Standard for Cabinets, Racks, Panels and Associated Equipment and accommodate industry standard 19" rack mount equipment.	
4.	Design	Front and Back doors should be perforated with atleast 63% or higher perforations.	
5.	Design	All racks should be OEM racks with Adjustable mounting depth, Multi-operator component compatibility, Numbered U positions, Powder coat paint finish and Protective grounding provisions.	
6.	Design	All racks should have mounting hardware 2 Packs, Blanking Panel.	
7.	Design	Keyboard Tray with BB Slides (Rotary Type) (1 no. per Rack)	
8.	Design	Stationery Shelf 627mm Network (2 sets per Rack)	
9.	Design	All racks must be lockable on all sides with unique key for each rack	
10.	Design	Racks should be compatible with floor-throw as well as top-throw data centre cooling systems.	
11.	Interface	Server Racks should have the following things in addition to the above-mentioned hardware <ul style="list-style-type: none"> • PS/2 Interface adapter • USB Interface adapter 	
12.	Cable management	Racks should have Rear Cable Management channels, Roof and base cable access	
13.	Cable management	Wire managers: Two vertical and four horizontal	
14.	Power distribution	<ul style="list-style-type: none"> • Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/13Amp Sockets), 	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> Electronically controlled circuits for Surge & Spike protection LED readout for the total current being drawn from the channel 32AMPS MCB 3KVAC isolated input to Ground & Output to Ground (1 No per Rack) 	
15.	Door	<ul style="list-style-type: none"> The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools. 	
16.	Fan trays	<ul style="list-style-type: none"> Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - 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 	
17.	Construction	<ul style="list-style-type: none"> Depth: 1000 mm Metal: Aluminium extruded profile Side panel: Detachable side panels (set of 2 per Rack) Width: 19" equipment mounting, extra width is recommended for managing voluminous cables 	

6.7.6 Network Rack

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design & Construction	Should be available in 2-Post Configurations Option of 84" or 96" height	
2.	Design & Construction	Should be available with an option of Rail Widths: 3", 6", 12" (2-Post)	
3.	Design & Construction	Load Capacity: 1000 lb (2 and 4-Post AI)	
4.	Design & Construction	EIA Standard Hole Pattern: 12-24 Threads @ 5/8" (127mm), 1/2" (25.4mm) Centres	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Design & Construction	Material: Al: 6061-T6 Aluminum Extrusion (3" Rail), Al: 6061-T6 0.125" Thick, (6" and 12" Rail), Steel: 14 Gauge (0.075 Thick), CRS	
6.	Design & Construction	Finish: Durable black epoxy powder-coat	
7.	Design & Construction	Hardware included	
8.	Cable Management	Ergonomically designed and aesthetically pleasing, Lightweight, but sturdy	
9.	Cable Management	Should have dual hinge latching door & can be opened right or left.	
10.	Cable Management	Cable fingers support up to 48 cables per RMU	
11.	Cable Management	Should be available in 6", 8", 10" & 12" vertical trough widths both single sided or double sided.	
12.	Cable Management	In case of Horizontal cable management, the cover should hinges up or down and locks into position with cylindrical finger ends for easy snap on installation	
13.	Cable Management	Horizontal cable management troughs should be available in 1, 2 & 3 RMU	
14.	Cable Management	Open back on 2U and 3U horizontal troughs for easy pass through of cables	
15.	Cable Management	Handle should be recessed to eliminate snag potential for clothes and arms	
16.	Cable Management	Should have C Channel bracket allowing for easy access to the cable trough	
17.	Cable Management	Provision for Tool-less installation of Cable Spool	
18.	Compliance	<ul style="list-style-type: none"> UL Listed, Certification - Information Technology and Communications equipment 	

6.7.7 Blade Chassis with Switch and virtual KVM

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Enclosure	Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit	
2.	Enclosure	The enclosure Should support full height/width and half height/width blades in the same enclosure, occupying a max of 10U rack height, it should support minimum 8 blade servers	
3.	Power	The enclosure should be populated fully with power supplies of the highest capacity & energy efficiency of platinum rating.	
4.	Power	The power subsystem should support N + N, N+1 power redundancy (where N is greater than 1) for a fully populated chassis with all servers configured with the highest CPU configuration (150 W and above),	
5.	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	
6.	Blade Support	Enclosure should support all Intel Xeon Scalable processors based 2 CPU and 4 CPU blades	
7.	Blade Support	Should support built-in management software in redundancy	
8.	Blade Support	Should provide single management console for all the blade servers across multiple chassis.	
9.	Converged Module	The chassis should be provided with redundant modules for connectivity	
10.	Converged Module	Chassis should have sufficient number of redundant 40gb based converged modules to provide a minimum FCOE uplink bandwidth of 20Gbps per blade server and 10Gbps sustained per blade server (with 1 module failure) for a fully populated chassis for converged Traffic.	
11.	Chassis Management software	Blade chassis management solution may be provided internal / external to the chassis and must provide single console for managing minimum up to 4 chassis for all associated components like Blade Servers, raid settings, NIC/HBA cards, IO Modules, Power supplies, Fans. Licenses to support the features to be supplied for fully populated chassis.	
12.	Chassis Management software	Centralized Redundant Management solution should be provided so that management of all blade servers across multiple chassis within Data Centre 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	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
13.	Chassis Management software	Should support auto-discovery of resources within an enclosure and on multiple connected enclosures.	
14.	Chassis Management software	Solution should support templates to quickly make changes to the infrastructure. the server BIOS version, MAC ID, NIC firmware version, WWPN, FC-HBA firmware version, Adapter QoS, Management module firmware version, UUIDs, Server Boot Policies, KVM IPetc. of the infrastructure required for workload	
15.	Chassis Management software	The management software should be used to create resource pools and have the blade resources assigned to the respective resource pools & re-assign resources to effectively utilize infrastructure	
16.	Chassis Management software	Role Based Access Control with at least 6 users to define roles and privileges and remote management capabilities including remote KVM should be included	

6.7.8 Internet Router

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes/No)
1.	Architecture	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 shall also support 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 shall run service & features as processes having full isolation from each other.	
2.	Architecture	The router shall support following interface: Gigabit Ethernet, STM1, STM16, STM64, 10G Ethernet, POS, E1, Channelized E1,	
3.	Performance	Backplane Architecture: The back-plane architecture of the router must be modular and redundant.	
4.	Performance	The routing aggregate throughput should be at least 5 Gbps which can scale up to 20 Gbps to meet future requirement without changing the hardware.	
5.	Performance	Should support minimum 8 Mbps and scalable up to 15 Mbps of forwarding performance	
6.	Performance	Router should have at least on-board/inbuilt 4GB DRAM on RP to handle routing and other processes. It should also support 1GB flash memory for configuration & OS backup.	
7.	Performance	-The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes/No)
		control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability.	
8.	Performance	-The router processor architecture must be multi-processor based and should support hardware accelerated and programmable IP forwarding and switching.	
9.	Performance	-The proposed router shall support VRFs	
10.	Performance	-The router shall support the IPv4 and IPv6 DUAL-stack in hardware and software.	
11.	Performance	-The router shall support minimum 768K IPv4 & IPv6 routes from day one (1) in FIB in future	
12.	Performance	-Shall have Multicast routes & IGMP groups.	
13.	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).	
14.	Protocol Support	The router should have support for 4,000 IPSEC tunnels and 1000 tunnels of GRE.	
15.	Protocol Support	Router shall support following MPLS features – LDP, Layer 2 VPN such as EoMPLS or equivalent with LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled.	
16.	QoS Features	The router shall support QoS policy in the router shall support 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.	
17.	QoS Features	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	
18.	Security Feature	The router shall support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT). The router shall support NAT6to4 function & vrf-aware NAT function.	
19.	Security Feature	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 shall support deep and stateful packet inspection to recognize a wide variety of applications using flows	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
20.	Security Feature	Router shall support IPsec (Internal/external) with at least 2 Gbps of IPSEC throughput	
21.	Management	The router shall support management through SNMPv1/v2/v3, support RADIUS and TACACS. The router shall 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 Packet Loss etc.	
22.	Interface Requirements:	Router shall be provided with 6 X 1 GE port with 2xSM & 4x1G copper transceivers& two 10G SR based Port	
23.	Compliance/ Certifications	The proposed router shall support IPv6	
24.	Compliance	The proposed router shall support IEEE 1588v2 standard.	

6.7.9 Core Router

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
1.	Architecture	Router should have redundant controller cards (redundant control plane) and should support stateful switchover, non-stop forwarding, Non-stop routing and Graceful restart.	
2.	Architecture	Router should be CE2.0/MEF14.0 certified/ compliant	
3.	Architecture	Router shall support MEF for Ethernet based services like PW, VPLS or ATOM.	
4.	Architecture	Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred	
5.	Architecture	The router shall support following type of interfaces – 10GE and 1GE interfaces.	
6.	Architecture	All the Ports and card on Router should be hot swappable and field replacement of port or card should not bring down the chassis.	
7.	Performance	Router shall support minimum non-blocking capacity of 40 Gbps with scalability of up to 60Gbps without changing the hardware	
8.	Performance	Router shall support 60 Mbps forwarding performance for IPv4 & IPv6 performance.	
9.	Performance	Router shall support 16000 Mac addresses	
10.	Performance	Router shall support 18000 IPv4 routes	
11.	Performance	router shall support 4000 queues and 128 MPLS VPN's	
12.	Performance	Router shall support aggregation of links. Minimum 8 links should be supported as part of single aggregation	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes/No)
13.	Performance	Router shall support IPSLA or equivalent and Y.1731 for performance monitoring	
14.	High Availability	Router should support Redundant Power Supply and should also support Online insertion and removal of same.	
15.	High Availability	Fan tray should be hot-swappable and should be a Field Replaceable Unit (FRU). The node can run indefinitely with a single fan failure. Shall Support hot-swappable for all modules. And secure normal operations when hot-swap event occurred	
16.	High Availability	Router shall support MPLS-TE with FRR for sub 50 msec protection.	
17.	High Availability	Router must support Traffic Engineering for node and link protection.	
18.	Protocol Support	Router shall support IPV4 and IPV6, IGMP V2/V3, Multicast Listener Discovery, IGMP and PIM, 6PE and 6VPE	
19.	Protocol Support	mode for IPV6 transport over IPV4, ECMP, LDP, BGP Prefix independent control (EDGE and Core) for IPV4 and IPV6, BGP, ISIS, OSPFv2 and V3, RSVP, VRRP and Traffic Engineering	
20.	Protocol Support	Router should support high availability for all BFD, BGP, OSPF and IS-IS and no packet loss during controller switch over.	
21.	Protocol Support	Router should support RFC 3107 of Carrying Label Information in BGP-4	
22.	Protocol Support	The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.	
23.	Protocol Support	Router shall support layer3 and layer2 MPLS VPN.	
24.	QoS Features	Router shall support HQOS on all kind of interface in both ingress and egress direction. Similar QOS shall be supported for all type of interface including Bundled interfaces.	
25.	QoS Features	Shall support Ingress classification, marking and policing on physical interfaces and logical interfaces using source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, MPLS EXP, DSCP,802.1p	
26.	QoS Features	Shall support Strict Priority Queuing or Low Latency Queuing to support real-time application like Voice and Video with minimum delay and jitter.	
27.	QoS Features	Congestion Management: WRED, Priority queuing, Class-based weighted fair queuing	
28.	Security & Management	Support 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. Should Support per-user Authentication,	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
		Authorization, and Accounting through RADIUS or TACACS and SNMPv1/v2/V3	
29.	Operating Environmental Requirements	0°C to 40°C operating temperature and 10 to 90%, non-condensing	
30.	Interface	The proposed router should be provided with the following minimum interfaces from day 1 . However, MSI should consider as per solution. - <ul style="list-style-type: none"> • 4x10G ports populated with minimum 2 X multimode transceiver and 1x10G SM transceiver • 4x1G SFP port • 4x 10/100/1000base-T Ethernet Ports. MSI to evaluate the final termination required as per their solution design and provide the required transceivers.	
31.	Compliance	The proposed router shall support IEEE 1588v2 standard.	

6.7.10 Spine Switch

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
1.	General	The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch.	
2.	General	The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.	
3.	General	The Switch should support non-blocking Layer 2 switching and Layer 3 routing. Switch with different modules should function line rate and should not have any port with oversubscription ratio applied	
4.	General	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch	
5.	General	Switch should support the complete STACK of IP V4 and IP V6 services.	
6.	General	Switch and optics must be from the same OEM	
7.	General	Switch should support non-blocking, wire speed performance per line card	
8.	Hardware and Interface	Minimum 32 nos. of line rate and Non - Blocking 40G ports populated with 8x40GBi-directional transceivers from day one and switch should have minimum one slots free for future	
9.	Hardware and Interface	Switch should have adequate power supplies for the complete system usage, providing N+1 redundancy	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes/No)
10.	Hardware and Interface	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/Link Aggregation Group (LAG) etc.	
11.	Hardware and Interface	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
12.	Performance	The switch should support 768KIPv4 routes or above	
13.	Performance	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG	
14.	Performance	Switch should support minimum 1000 VRF or equivalent instances	
15.	Performance	Switch should support total aggregate minimum 8 Tbps minimum of switching capacity considering future scalability	
16.	Virtualization	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890	
17.	Virtualization	Switch should support VXLAN (RFC7348) and EVPN control plane	
18.	Virtualization	Switch must support VXLAN Switching/Bridging and/or VXLAN Routing without any performance degradation and MSI should implement VXLAN switching/routing in their design architecture	
19.	Layer 2	Switch should support minimum 92,000 no. of MAC addresses	
20.	Layer 2	Switch should support Jumbo Frames up to 9K Bytes on 40G Ports	
21.	Layer 2	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
22.	Layer 3	Switch should support Policy based routing	
23.	Layer 3	Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Support RFC 3618 Multicast Source Discovery Protocol (MSDP) d. IGMP V.1, V.2 and V.3	
24.	Layer 3	Switch should support Multicast routing	
25.	Availability	Switch should support for BFD For Fast Failure Detection	
26.	Quality of Service	Switch should have a minimum buffer of 80 Mb	
27.	Security	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
28.	Security	Switch should support for external database for AAA using: a. TACACS+	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
		b. RADIUS	
29.	Security	Should support Standard & Extended ACLs	
30.	Security	Switch should support MAC ACLs	
31.	Manageability	Switch should support for predefined and customized execution of script for device manage for automatic and scheduled system status update for monitoring and management	
32.	Manageability	Switch should provide different privilege for login in to the system for monitoring and management	
33.	Manageability	All relevant licenses for all the above features and scale should be quoted along with switch	
34.	Redundancy	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy	

6.7.11 Leaf (TOR) Switch

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
1.	Solution Requirement	The Switch should support non-blocking Layer 2 switching and Layer 3 routing	
2.	Solution Requirement	There switch should not have any single point of failure like power supplies and fans etc. should have 1:1/N+1 level of redundancy	
3.	Solution Requirement	Switch and optics must be from the same OEM	
4.	Solution Requirement	Switch should support the complete STACK of IP V4 and IP V6 services.	
5.	Hardware and Interface	Switch should have the following interfaces: a. 48 X 1G/10G/25G Interface with 32x10G SR Transceiver b. 6 X 40GbE QSFP ports populated with 2x40G bidi transceiver for Spine connectivity;	
6.	Hardware and Interface	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc.	
7.	Hardware and Interface	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy	
8.	Performance	The switch should support 12,000 IPv4 and IPv6 routes entries in the routing table including multicast routes	
9.	Performance	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG	
10.	Performance	Switch should support full duplex wire rate switching capacity	
11.	Performance	Switch should support minimum 1000 VRF or equivalent instances	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
12.	Performance	Each leaf should have connectivity to all spine switches over 40Gbps minimum	
13.	Advance Features	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348) and MSI should implement VXLAN in their design architecture	
14.	Advance Features	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data Centre and should be implemented	
15.	Advance Features	Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation	
16.	Layer2	Switch should support minimum 92,000 no. of MAC addresses	
17.	Layer2	Switch should support Jumbo Frames up to 9K Bytes on all Ports	
18.	Layer2	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities	
19.	Layer3	Switch should support Policy based & segment routing	
20.	Layer3	Switch should provide multicast traffic reachable using: a. PIM-SM b. PIM-SSM c. Bi-Directional PIM d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP) e. IGMP V.1, V.2 and V.3	
21.	Layer3	Switch should support Multicast routing	
22.	Layer3	Switch should support for BFD For Fast Failure Detection	
23.	Quality of Service	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x and should have a minimum buffer of 20MB	
24.	Security	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy	
25.	Security	Switch should support for external database for AAA using: a. TACACS+ b. RADIUS	
26.	Security	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined	
27.	Security	Should support Standard & Extended ACLs; it should also support MAC ACLs	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes/No)
28.	Manageability	Switch should support for predefined and customized execution of script for device manage for automatic and scheduled system status update for monitoring and management	
29.	Manageability	Switch should support Real-time Packet Capture using Wireshark in real-time for traffic analysis and fault finding	
30.	Manageability	All relevant licenses for all the above features and scale should be quoted along with switch	

6.7.12 Fabric Manager

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The MSI shall use hardware/software fabric manager/software Network Virtualization in complementary manner for providing secure and seamless underlay and overlay networking within the IT infrastructure as per their solution design.	
2.	General	Fabric is the Clos Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol	
3.	General	Fabric should have following functionalities to be achieved:	
4.	General	Flexibility: allows workload mobility anywhere in the DC	
5.	General	Robustness: while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone	
6.	General	Performance: full cross-sectional bandwidth (any-to-any)– all possible equal paths between two endpoints are active	
7.	General	Deterministic Latency: fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale	
8.	General	Scalability: add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.	
9.	Fabric	In the fabric the oversubscription ration of the connectivity between each leaf to SPINE switches should not be less than 4:1	
10.	Fabric	Fabric must support various Hypervisor encapsulations including VXLAN and 802.1q natively without any additional hardware/software or design change.	
11.	Fabric	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.	
12.	Fabric	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
13.	Fabric	Fabric Spine switches should only connect to the leaf switches	
14.	Fabric	Fabric must integrate with different virtual machine manager and manage virtualize networking from the single pane of Glass - Fabric Manager/SDN Controller	
15.	Fabric	Fabric must integrate with best of breed L4 - L7 appliances and manage using single pane of glass - Fabric Manager/SDN Controller	
16.	Fabric	Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.	
17.	Fabric Layer 2, Layer 3and Misc	Fabric must support Layer 2 features like LACP, STP /Rapid Spanning Tree Protocol /Multiple Spanning Tree Protocol, VLAN Trunking, LLDP etc.	
18.	Fabric Layer 2, Layer 3and Misc	Fabric must support Jumbo Frame up-to 9K Bytes on 1G/10G/25G/40G ports	
19.	Fabric Security	Fabric must support VM attribute based zoning and policy directly / via integration to orchestration layer / other means	
20.	Fabric Security	Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment directly / via integration with orchestration layer / other means	
21.	Fabric Scale and Performance	Fabric should support scale up and scale out without any service disruption	
22.	Fabric Scale and Performance	Fabric must be capable of connecting 50 physical servers and scale to 500 physical servers.	
23.	Fabric Scale and Performance	Fabric must support minimum of 4 Leaf switches and scale up to 50 Leaf switches without any design change.	
24.	Fabric Scale and Performance	Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change	
25.	Fabric Scale and Performance	Fabric must scale from 1 Tenant to 32 Tenant without any additional component or upgrade or design change	
26.	Fabric Scale and Performance	Fabric must support minimum of 2 Spine Switches and scale up-to 6 Spine switches without any design change.	
27.	Fabric Management	Fabric must provide Centralized Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric.	
28.	Fabric Management	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralized Management appliance or SDN Controller.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
29.	Fabric Management	Centralized management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.	
30.	Fabric Management	Centralized management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.	
31.	Fabric Management	Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric.	

6.7.13 Internet Firewall

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Hardware Architecture	The appliance based security platform should provide firewall, Application Control, Malware Protection and IPS functionality (on one /multiple appliances)	
2.	Hardware Architecture	The appliance should have minimum 8x1/10G port switch multi-mode transceiver from day one	
3.	Hardware Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory	
4.	Hardware Architecture	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.	
5.	Performance & Scalability	Solution should support minimum 4 Gbps of NGFW / Threat Prevention real-world / production performance	
6.	Performance & Scalability	Firewall should support at least 18,00,000 concurrent sessions with application visibility turned on	
7.	Performance & Scalability	Firewall should support at least 25,000 connections per second with application visibility turned on	
8.	Performance & Scalability	Firewall should support Active-Standby/ Active-Active high availability deployment modes.	
9.	Performance & Scalability	Firewall should have integrated redundant hot-swappable power supply	
10.	Performance & Scalability	Firewall should have integrated redundant hot-swappable fan trays/ Modules	
11.	Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, URL, zones, VLAN, etc.	
12.	Firewall Features	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
13.	Firewall Features	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
14.	Firewall Features	Should support Multicast protocols like IGMP, PIM, etc.	
15.	Firewall Features	Should support capability to integrate with other security solutions to receive contextual information	
16.	Firewall Features	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness	
17.	Firewall Features	Should support more than 4000 (excluding custom signatures) IPS signatures or more	
18.	Firewall Features	Should be capable of supporting at least 60-70 number of URL filtering categories	
19.	Firewall Features	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
20.	Firewall Features	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
21.	Firewall Features	Should be capable of detecting and blocking IPv6 attacks.	
22.	Firewall Features	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
23.	Firewall Features	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
24.	Firewall Features	Solution shall have capability to analyse and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, and FTP	
25.	Firewall Features	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
26.	Firewall Features	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques.	
27.	Firewall Features	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly	
28.	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
29.	Management	The management appliance should have 2 X 1G port and integrated redundant power supply from day one	
30.	Management	The management platform must be able to store record of 15000 user or more	
31.	Management	The management platform must provide a highly customizable dashboard.	
32.	Management	The management platform must domain multi-domain management	
33.	Management	The management platform must provide centralized logging and reporting functionality	
34.	Management	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
35.	Management	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
36.	Management	The centralized management platform must not have any limit in terms of handling logs per day	
37.	Management	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
38.	Management	The management platform support running on-demand and scheduled reports	
39.	Management	The management platform must provide risk reports like advanced malware, attacks and network threats	

6.7.14 Internal Firewall

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Hardware Architecture	The appliance based security platform should provide firewall, Application Control and IPS functionality (on one/multiple appliances)	
2.	Hardware Architecture	The appliance should support at least 4x1G Ethernet Ports & 4 X 10G ports with multi-mode transceiver from day one	
3.	Hardware Architecture	The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system to support higher memory	
4.	Performance & Scalability	Should support 6 Gbps of (NGFW / Threat Prevention) real-world / production performance	
5.	Performance & Scalability	Firewall should support at least 25,00,000 concurrent sessions with application visibility turned on	
6.	Performance & Scalability	Firewall should support at least 35,000 connections per second with application visibility turned on	
7.	Performance & Scalability	Firewall should support Active-Standby/ Active-Active/Clustering high availability deployment modes.	
8.	Performance & Scalability	Firewall should have integrated redundant hot-swappable power supply	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Performance & Scalability	Firewall should have integrated redundant hot-swappable fan tray / modules	
10.	Firewall Features	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application url, zones, vlan, etc.	
11.	Firewall Features	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality	
12.	Firewall Features	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6	
13.	Firewall Features	Should support Multicast protocols like IGMP, PIM, etc.	
14.	Firewall Features	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names	
15.	Firewall Features	Should support more than 4000 (excluding custom signatures) IPS signatures or more	
16.	Firewall Features	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.	
17.	Firewall Features	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.	
18.	Firewall Features	Should be capable of detecting and blocking IPv6 attacks.	
19.	Firewall Features	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control	
20.	Firewall Features	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor	
21.	Firewall Features	Solution should support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist	
22.	Firewall Features	The Appliance OEM must have its own threat intelligence analysis Centre and should use the global footprint of security deployments for more comprehensive network protection.	
23.	Firewall Features	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).	
24.	Firewall Features	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. I	
25.	Firewall Features	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP	
26.	Management	The management platform must be accessible via a web-based interface and ideally with no need for additional client software	
27.	Management	The management appliance should have 2 X 1G port and integrated redundant power supply from day one	
28.	Management	The management platform must be able to store record of 15000 user or more	
29.	Management	The management platform must provide a highly customizable dashboard.	
30.	Management	The management platform must domain multi-domain management	
31.	Management	The management platform must provide centralized logging and reporting functionality	
32.	Management	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.	
33.	Management	Should support troubleshooting techniques like Packet tracer and capture	
34.	Management	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.	
35.	Management	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).	
36.	Management	The centralized management platform must not have any limit in terms of handling logs per day	
37.	Management	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.	
38.	Management	The management platform support running on-demand and scheduled reports	
39.	Management	The management platform must provide risk reports like advanced malware, attacks and network threats	

6.7.15 Server & Link Load balancer and Web Application firewall and DDoS

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The proposed appliance should provide integrated functionalities of Server Load balancer, Intelligent DNS, Link Load Balancing, SSL Offloading, WAF and Fraud Protection (Application Layer Encryption).	
2.	General	The proposed appliance must provide 8 X 1 G ports and 4 X 10 G SFP+ ports	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	The proposed appliance should provide minimum throughput of 5 Gbps	
4.	General	The proposed appliance must support minimum SSL TPS of 9k (RSA 2k keys) and minimum 6K (with ECDSA 256 key).	
5.	General	The proposed appliance should support minimum 5 Gbps Compression throughput	
6.	General	The proposed appliance should support minimum 5 Gbps of SSL throughput	
7.	General	The proposed solution should support minimum 400K DNS Query Per Second	
8.	General	While applications are deployed in private DC and public cloud, the proposed application security architecture should have a mechanism of centralized Security policies enforcement, SSL Certificates management for workloads on Private DC and public clouds.	
9.	Availability features	The proposed solution must be able to load balance both TCP and UDP based application from L2 to L7 including lightweight IoT protocols like MQTT and CoAP protocol for machine to machine connectivity between IoT appliances such as small sensors, mobile devices etc.	
10.	Availability features	The proposed solution must be able to perform TCP multiplexing, TCP queuing, buffering and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, hardware based compression, caching in active-passive mode.	
11.	Availability features	The proposed solution must offer out of band programming for control plane along with data plane scripting for functional like content inspection and traffic management	
12.	Availability features	The proposed solution must support global server load balancing between DC and DR	
13.	Availability features	Device should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	
14.	Availability features	The proposed solution must support policy nesting at layer 4 and layer7 to address the complex application integration. Further it should also provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	
15.	Security Functionalities	The proposed solution must provide comprehensive security both at network and application level via WAF and Application Layer Encryption from Day 1.	
16.	Security Functionalities	Geolocation IP address database to identify the source of the attack origin and IP Reputation	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		Mechanism to identify the Blacklisted TOR Networks or Proxy IP address to Block the request immediately.	
17.	Security Functionalities	Should support Web socket and Secure Web socket traffic inspection.	
18.	Security Functionalities	System should be able to encrypt the user credentials in real-time so as to protect the credentials especially password or any other sensitive parameter as defined by department to protect from key loggers and credential stealing malware residing in the end user's system	
19.	Security Functionalities	New modules of applications should be learnt dynamically, and WAF should also provide the option of deploying the rules learnt dynamically for these new modules without manual intervention.	
20.	Security Functionalities	Must be able to take threat intelligence feed to reveal inbound communication with malicious IP addresses, and enable granular threat reporting and automated blocking.	
21.	Security Functionalities	Support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	
22.	Security Functionalities	System should be stable and not affect service availability even upon any system fault	
23.	Security Functionalities	Solution should perform comprehensive countermeasure to protect against zero-day attack, Challenge – Response Mechanism, which should be able to detect and protect attacks in real-time through inbuilt Captcha Mechanism	
24.	Security Functionalities	Solution should integrate with AD, LDAP, Radius, TACACS with inbuilt OTP mechanism for 2 Factor Authentication in future.	
25.	DNS and Link Load Balancing	Must be intelligent DNS which can check health of server and resolve based on Availability of server at Primary Datacentre or Secondary Datacentre	
26.	DNS and Link Load Balancing	Must support Zone files, Subdomain Delegation	
27.	DNS and Link Load Balancing	Must support DNS master or slave role per zone file	
28.	DNS and Link Load Balancing	Must support DNSSEC with auto key rollover	
29.	DNS and Link Load Balancing	Should support automatic Zone file synchronization between master and slave	
30.	DNS and Link Load Balancing	Should be able to provide inbound load balancing using DNS mechanism where the load balancer replies the DNS responses as per the link availability and load balancing policy and load on each link	
31.	Management, Reporting and Other	Proposed solution should be manageable from a single management platform	

6.7.16 Web Security Appliance

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	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.	General	The appliance based Solution should be provided with hardened Operating System.	
3.	General	The underlying operating system and hardware should be capable of supporting with 1000 users with licenses and MSI should include 200 user licenses from day one	
4.	General	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.	
5.	General	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	
6.	General	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.	
7.	General	Should support active/active High Availability mode	
8.	General	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.	
9.	General	The solution should have the capability of analysis zero-day attacks on day 1. The sandboxing solution should seamlessly integrate with the web proxy and facilitate multiple levels of analysis to identify all threats.	
10.	General	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.	
11.	General	The web proxy solution should be capable of executing the web sessions from un-categorised websites in a local container away from the endpoint thereby preventing any website delivered zero-day malwares from reaching the endpoints	
12.	General	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action	
13.	General	Should support the functionality to block applications that attempts to tunnel non-HTTP traffic on ports typically used for HTTP traffic.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
14.	General	Should support the functionality for blocking non-SSL traffic on SSL ports & should also support the functionality to tunnel the transaction.	
15.	General	The solution should act as an FTP proxy and enable organizations to exercise granular control, including: allow/block FTP connections, restrict users/groups, control uploads/downloads, and restrict sent/received files to certain types or sizes.	
16.	General	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.	
17.	General	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	
18.	General	The solution should support granular application control over web e.g. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.	
19.	General	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.	
20.	General	The solution should provide Web Reputation Filters that examine every request made by the browser (from	
21.	General	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.	
22.	General	The Web Reputation Filters should have capability to analyze more than 100 different web traffic	
23.	General	Network-related parameters to accurately evaluate the trustworthiness of a URL or IP address.	
24.	General	Solution should also support in participating by providing information to the cloud based servers to increase the efficacy & reputation based scoring.	
25.	General	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.	
26.	General	The solution should have an inbuilt URL filtering functionality with multiple pre-defined categories.	
27.	General	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organization.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
28.	General	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.	
29.	General	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.	
30.	General	The solution should have facility for End User to report Mis-categorization in URL Category.	
31.	General	Support portal should give facility to end user to check URL category and submit new URL for categorization	
32.	General	Solution should support filtering adult content from web searches & websites on search engines like google.	
33.	General	Solution should support following end user notification functionalities.	
34.	General	The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.	
35.	General	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.	
36.	General	The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.	
37.	General	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.	
38.	General	The Support Engineers should be able to login to appliance using secure tunneling methods such as SSH for troubleshooting purposes	
39.	General	The appliance should provide seamless version upgrades and updates.	
40.	General	The appliance should be manageable via HTTP or HTTPS, command line using SSH	
41.	General	The appliance should be manageable via command line using SSH	
42.	General	Solution should support automatic "rollover" & archive the log file when it reaches admin defined maximum file-size or time interval like daily/weekly rollover of logs.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
43.	General	The appliance should support following mechanism to transfer log files:	
44.	General	Should support remote FTP client to access the appliance to retrieve log files using an admin or operator user's username and password.	
45.	General	Reports on Bandwidth Consumed / Bandwidth Saved	

6.7.17 Network Behaviour Analysis

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Solution should be capable of performing network behaviour analysis along with continuous full packet capture and forensics capabilities. Should capture all packets from network in real-time and be able to classify, extract and analytics, reconstructs network activity and forensics over IPv4 and, IPv6	
2.	General	Ability to import PCAP & PCAPNG files simultaneously while the live capture is going on. making it easy to analyze historical data or, captures from other sources. The solution should also include a packet viewer that is capable of following TCP streams.	
3.	General	Should capture all packets from network in real-time and be able to classify, extract and analytics, reconstructs network activity and forensics over IPv4 and, IPv6	
4.	General	Should Identify the source of an attack and should not block legitimate users	
5.	General	Solution should have capability of retrieval of relevant packets to a cyber-security incident	
6.	General	Solution should perform lossless packet capture at rate of 1 Gbps of network traffic	
7.	General	Support importing/ exporting archived raw packets/files for analysis	
8.	General	Solution should Index all the data in the packets to simplify navigation across data silos and enable search-driven data discovery of packet metadata AND content for incident analysis	
9.	General	3rd Party Threat Feed integration – add live-feeds, like Snort, quickly and easily. Reputation Services provide added value and threat intelligence	
10.	General	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.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
11.	General	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.	
12.	General	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	
13.	General	The solution must have feature for root cause analysis and while PCAP import the System is performing LIVE packet capture of the network	
14.	General	Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.	
15.	General	Should support the capability to link usernames to IP addresses for suspected security events. Should be able to remediate user's Endpoints from the same console	
16.	General	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.	
17.	General	Provide a visual representation of relationships between entities (IP, email ids, etc)	
18.	General	The reporting should be integrated with other network security systems (IPS, IDS, Network Access Control (NAC), and Firewall etc.).	
19.	General	Solution should support capability to quarantine / remediate endpoint	
20.	General	Solution should be able to identify potential DDOS attacks originating from behind proxies.	
21.	General	Solution should be able to identify anomalies related to VOIP protocols over data network	
22.	General	Root Cause Explorer Features - Automates tracing of HTTP referrer chains that can significantly reduce time to search for related preceding sessions.	
23.	General	Solution should support access to raw as well as processed logs	
24.	General	Dashboard should have the facility to be configured according to user profile	
25.	General	System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues	
26.	General	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
27.	General	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.	
28.	General	The solution should support the identification of applications tunnelling on other ports	
29.	General	Solution should be able to collect security and network information of servers and clients without the usage of agents	
30.	General	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance	
31.	General	The solution should have the ability to state fully reassemble uni-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry	
32.	General	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.	General	Dashboard should have the facility to be configured according to user profile	
34.	General	Solution should probe the network in a manner so that impact on network performance is minimal.	
35.	General	Ability to create new rules that applies to all previously captured data without the need to re-ingest older captured data to get the Application Rule to create a new piece of meta data	
36.	General	The tool should have a system for interactive event identification and rule creation	
37.	General	The solution should support - classification from more than 2,800 protocols/applications (natively without writing any custom parsers) and thousands of descriptive, metadata attributes, including content types, file names, and more - for easy analysis and recall without writing any custom parsers.	
38.	General	Solution should have facility to assign risk and credibility rating to events.	
39.	General	Solution should support traffic rate up to 1 Gbps	
40.	General	Proposed solution should be a dedicated appliance based solution provisioned with dedicated storage of at least 300 TB. This solution should not be a part of firewall, IPS, SIEM and should not be a server based solution.	

6.7.18 12-Port Layer 3 10G Switch (For Interconnecting)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Switch Should have 12 numbers of 10GSFP+ ports populated with multi-mode modules	
2.	General	Should have Internal Redundant Power supply	
3.	General	Switch should be based on a Modular OS Architecture	
4.	General	Switch should have USB for OS Management (uploading, downloading & booting of OS and Configuration).	
5.	General	Switch should have Multicore CPU Architecture.	
6.	General	Should have at least 4GB of Flash for storing OS and other Logs and 4GB DRAM	
7.	General	Switch should have Front to Back Airflow system and 3 number of field replaceable FAN's. In case of failure of one fan then other Fans should automatically speed-up	
8.	General	Switch should have power savings mechanism wherein it should reduce the power consumption on ports not being used.	
9.	General	Switch should be Rack Mountable and should not take space more than 1RU	
10.	Performance	Forwarding rate – 210 Mbps at least	
11.	Performance	Configurable at least 32000 MAC addresses	
12.	Performance	Should support at least 24K Ipv4 Routes	
13.	Stacking/virtual chassis	Switch should have dedicate stacking port and should support at least 8 number of switches in a single stack	
14.	Stacking/virtual chassis	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.	
15.	Stacking/virtual chassis	The Switch stacking module/interfaces should be hot-swappable.	
16.	Stacking/virtual chassis	The Switch stacking should support 320 Gbps of throughput.	
17.	Stacking/virtual chassis	The Switch stacking should support automatic upgrade when master switch receives a new software version.	
18.	Layer 3	The Switch should support routing protocols such OSPF, BGPv4, IS-ISv4	
19.	Layer 3	The Switch should support IP Multicast routing protocol i.e. PIM, PIM Sparse Mode, PIM Dense Mode, PIM Sparse-dense Mode & Source-Specific Multicast	
20.	Layer 3	The Switch should have basic IP Unicast routing protocols (static, RIPv1 & RIPv2) and VRRP	
21.	Layer 3	The Switch should have IPv6& IPv4 Policy Based Routing (PBR) and Inter VLAN Routing	
22.	Layer 2	The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighbouring device giving the	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		details about the platform, IP Address, Link connected through etc. thus helping in troubleshooting connectivity problems.	
23.	Layer 2	The Switch should support centralized VLAN Management, VLANs created on the core switch should be propagated automatically.	
24.	Layer 2	The Switch should support 802.3ad (LACP) to combine multiple network links for increasing throughput and providing redundancy.	
25.	Network Security	The Switch should have Port security to secure the access to an access or trunk port based on MAC address to limit the number of learned MAC addresses to deny MAC address flooding.	
26.	Network Security	The Switch should support Dynamic ARP inspection (DAI) to ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP.	
27.	Network Security	The Switch should support IP source guard to prevent a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.	
28.	Network Security	The Switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass, and web authentication using a single, consistent configuration.	
29.	Network Security	The Switch should support Private VLANs to restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a no broadcast multi-access like segment to provide security & isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.	
30.	Network Security	The Switch should support IPv6 RA Guard, DHCPv6 guard, IPv6 Snooping to prevent any Man-in-middle attack.	
31.	Operational	The Switch should support dynamic port and session configuration management.	
32.	Quality of Service	The Switch should support IP SLA feature set to verify services guarantee based on business-critical IP Applications.	
33.	Operational	The Switch should support Auto QoS for certain device types and enable egress queue configurations.	
34.	Operational	The Switch should support Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.	
35.	Application visibility	The Switch should support at-least 24000 Flows per switch	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
36.	Certification	Switch should be EAL3/NDPP Certified	

6.7.19 24-Port PoE GE layer 2 Switch

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Hardware and Interface	Switch should have minimum 24x10/100/1000Mbps PoE/PoE+ Ethernet Ports and 4x1G/10G SFP uplink ports.	
2.	General Hardware and Interface	Switch shall support minimum 80 Gbps of stacking bandwidth and stacking port should be dedicate port not uplink port	
3.	General Hardware and Interface	Switch should support Redundant Power supply (Internal/External)	
4.	General Hardware and Interface	Stacking module should be hot-swappable.	
5.	Performance	Switch shall have minimum 216 Gbps of switching fabric and 70 Mbps of forwarding rate.	
6.	Performance	Switch shall have minimum 16 K MAC Addresses.	
7.	Performance	Switch shall have minimum 1K Active VLANs.	
8.	Performance	Switch shall support minimum 1K IPv4 and IPv6 unicast routes.	
9.	Performance	Switch shall support minimum 1K IPv4 and IPv6 multicast groups.	
10.	Performance	Switch shall support minimum 500 IPv4 and IPv6 QoS and Security ACLs.	
11.	Performance	Switch must have at least 512 Mb RAM and 128Mb Flash memory	
12.	IEEE Standards	Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.	
13.	Quality of Service (QoS) requirements	Switch shall have 802.1p class of service, IP differentiated service code point (DSCP) and QoS.	
14.	Quality of Service (QoS) requirements	Switch shall have committed information rate, rate limiting and flow based rate limiting.	
15.	Quality of Service (QoS) requirements	Switch shall have minimum 8 egress queues per port and strict priority queuing.	
16.	System Management and Administration	Switch should support SSHv2, SNMPv2c, SNMPv3, NTPv3 and NTPv4.	
17.	System Management and Administration	Switch should support AAA using RADIUS and TACACS+.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
18.	System Management and Administration	Switch should support port security, DHCP snooping, Dynamic ARP inspection, IP Source guard, BPDU Guard, Spanning tree root guard and IPv6 First Hop Security.	
19.	System Management and Administration	Switch should support software upgrades via TFTP or FTP.	
20.	System Management and Administration	Switch should support IPv4 and IPv6 ACLs, VLAN, Port and Time-based access list with time ranges.	
21.	System Management and Administration	Switch shall have Switch Port Analyzer (SPAN) and Remote Switch Port Analyzer (RSPAN).	
22.	System Management and Administration	Switch shall have trace route for ease of troubleshooting by identifying the physical path that a packet takes from source to destination.	
23.	System Management and Administration	Switch shall have Internet Group Management Protocol (IGMP) Snooping for IPv4 and IPv6, Multicast Listener Discovery v1 and v2 Snooping and Multicast VLAN Registration protocol/PIM.	
24.	System Management and Administration	Switch shall have per port broadcast, multicast and unicast storm control.	
25.	Regulatory Compliance	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.	
26.	Regulatory Compliance	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.	

6.7.20 Authentication, Authorization and Accounting (AAA) Specification

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
27.	General	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture, profiling and guest management services on a single platform.	
28.	General	Solution should include all required licenses to perform above mentioned capabilities for 100 endpoints from day one and scalable to 5,000 in future. Additionally, 400 endpoints licenses to be provided for AAA & Guest management only	
29.	General	It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
30.	General	Proposed solution should include two appliances to be configured in Active/Standby	
31.	General	Proposed solution should integrate with Firewall so that they learn identity information from access devices	
32.	General	Should support enforcing security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention	
33.	General	Should support improve network access control capabilities to identify, mitigate/quarantine and rapidly contain threats	
34.	General	Should utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).	
35.	General	Should provide a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect	
36.	General	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, IoT and tablets.	
37.	General	It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.	
38.	General	The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.	
39.	General	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.	
40.	General	<p>Solution should support the following endpoint</p> <ul style="list-style-type: none"> • Checks for compliance for windows endpoints: • Check process, registry, file & application • Check operating system/service packs/hotfixes • check for Antivirus installation/Version/ Antivirus Definition Date 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> check for Antispyware installation/Version/ Antispyware Definition Date Check for windows update running & configuration 	
41.	General	Proposed solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices	
42.	General	TACACS+ device administration should support: <ol style="list-style-type: none"> 1. Role-based access control 2. Flow-based user experience 3. Per Command level authorization with detailed logs for auditing 	
43.	General	Proposed solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number	
44.	General	Proposed solution should support capability to create different network device groups so that administrator can create: <ol style="list-style-type: none"> 1. Different policy sets for IOS/OS or wireless controller OS 2. Different for firewall 3. Differentiate base on location of device 	
45.	General	Proposed solution should be able to create TACACS+ profile like Monitor, Privilege level, default, etc. to control the initial login session of device administrator.	
46.	General	Proposed solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, (any character), X (matches any), etc. and support stacking as well	
47.	General	Proposed solution must support TACACS+ in IPv6 network	
48.	General	Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.	
49.	General	Should support troubleshooting & Monitoring Tools	

6.7.21 SMS Gateway

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Bidder shall provide SMS gateway of Telecom Service provider which has ability to withstand for continued growth in A2P SMS and support SVI_SMSG	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	General	The SMS gateway PULL SMS application must have security features to ensure confidentiality of sensitive customer data.	
3.	General	The SMS gateway PULL SMS application should be able to retrieve SMSs sent by devotees to one or more short codes / virtual numbers.	
4.	General	The SMS gateway PUSH SMS application should be able to send messages at different priority levels. In case the total number of messages to be sent exceeds the capacity promised, messages should be sent first as per higher priority and then following a FIFO rule. Other messages must be en-queued.	
5.	General	The SMS gateway PUSH SMS application must have the ability to set working hours and working days.	
6.	General	The Solution should offer configurable mechanism in terms of number of retries & time duration for each retry for messages that could not be delivered immediately.	
7.	General	Online Mechanism in real-time mode shall be provided for SLA enforcement with regard to Uptime of Push /Pull services & Delivery of Push SMS along with flexibility to generate MIS on daily/weekly/fortnightly/monthly/specified date range basis.	
8.	General	The bidder should integrate with the Dashboard/Website/Portal for Administration features like monitoring of total messages sent within a day/ week/ month, time delay (if any) in sending the messages, no of failed messages (with reasons for failure), invalid mobile numbers, No of Push & Pull Messages sent.	
9.	General	The successful bidder shall demonstrate the Dashboard functionality & Reports format to SKVT before commissioning of SMS gateway services.	
10.	General	The bidder shall ensure that SMS whose contents exceeds 160 characters, should be delivered as a single message on receiver's handset.	
11.	General	The bidder should have proper test infrastructure with capability of end to end testing of all integration with SKVT Applications.	
12.	General	Check should be properly imposed to avoid Duplicate/ Multiple SMS Delivery to customers.	
13.	General	The solution should be capable of generating detailed report in Excel/ PDF. The solution should be capable of providing mobile-wise, Date-wise, category-wise reports and aggregated reports per category. The reports should contain timestamps of SMS received at Bidder's server, SMS Sent to the Telecom Operator,	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		actual delivery to the end user & final status of SMS alert along with status description	

6.8 Generic IT Hardware

6.8.1 Keyboard and Joystick

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The control board shall be based upon standard components and proven technology	
2.	Controller	Shall be equipped with Keypad for selecting desired cameras/ as per user configurations	
3.	General	Shall be equipped with Jog dial for Viewing recording.	
4.	Technical	Joystick: Pan Tilt and Zoom function	
5.	Interface	USB 1.1/2.0/3.0 compliant	
6.	Power	Via USB	
7.	General	The control board shall be of modular design and provide keypad, joystick and jog dial functionality	
8.	General	The inter-connectable modules shall be backed by an open and published API and shall, when combined with a video management application	
9.	Keypad	Shall be equipped with 22 keys: 10 application defined hotkeys of which 5 are backlit, 0-9, TAB, ALT	
10.	Jog dial	6 application defined hotkeys	
11.	Joystick	Hall-effect joystick with three axis: a. X/Y: for pan and tilt b. Z: knob for zoom c. 6 application defined hotkeys	
12.	General	The following features to be available; vector-solving, with twisting, return to-centre head	
13.	Operating Cycle for Joystick	> 5,000,000 cycles or better	
14.	Deflection	Square delimiter Pan/Tilt (XY): $\pm 15^\circ$ Zoom (Z): $\pm 25^\circ$	
15.	Casing	Polycarbonate	
16.	Compatibility	Shall support all cameras and video servers	
17.	Operating System Supported	Windows 7 or Later or Any other Operating system	
18.	Certification	EN, CE, FCC, IEC	
19.	Operating conditions	0 °C to 60 °C	
20.	Operating Humidity	20% to 80% (RH)	

6.8.2 Video Wall

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Video wall	50 inch Cubes (LED Based projection)- Two setups of 4X2 matrix each	
2.	Technology	Single chip DLP Technology	
3.	Resolution	1920x1080	
4.	Brightness	240 Cd/m ² or better	
5.	On-screen contrast	1,200,000:1 (dynamic) or better	
6.	Display technology	DLP rear projection with DMD Chip	
7.	Colour gamut	>15 mill	
8.	Brightness uniformity	>90% or better	
9.	Screen	180° viewing angle screen	
10.	Screen Gap	Less than 1 mm at ambient temperature in Control room	
11.	Colour stability	Self-calibration with advanced colour sensor	
12.	Dimensions	Diagonal: 50 "	
13.	Light source	LED - 6x redundancy	
14.	Light source	System should also automatically switch back to primary DVI input from HDMI input as soon as the primary DVI input is available again.	
15.	Light source lifetime	> 60,000h Typical usage mode	
16.	Light source lifetime	> 80,000h Economy usage mode	
17.	Control BD Input terminals	Input: 2 xDigital DVI Input: 1 xHDMI Input: 1 xHD-BaseT Input: 1 xDisplay Port Output: 1 X Digital DVI	
18.	Conditions for operation	10°C-40°C, 80% humidity (Non- Condensing)	
19.	Input voltage	90 – 240 V, 50-60Hz	
20.	Signal input/output	Single I link DVI in / Single link DVI out	
21.	Direct Ethernet access	IP control	
22.	Graphical user interface	All settings and operational parameters	
23.	Third party interface	Should be open to third party interface	

6.8.3 Video Wall Controller

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	CPU Processing	Intel® Core™ i7 Quad Core 3.0 GHz processor or better	
2.	Memory	16 GB RAM	
3.	Hard disk	2x 600 GB RAID-1, Hot-plug redundant	
4.	Optical drive	DVD R/W	
5.	Network	2x1 Gb/s LAN	
6.	System backplane	PCI express 3.0 backplane (min 10 slots)	
7.	Graphics card	- Support for 4 Ch Graphic card with DVI outputs- Should support Display Port (max resolution: 2560x1600@60Hz) - 1920x1200@60 Hz (DVI)	
8.	Input	Supporting 10 nos. DVI, Dual LAN, RGB Signals	
9.	Output	12 DP/DVI outputs to the cubes	
10.	Dimensions	19" Rack mount	
11.	Power Supply	100-240VAC, 50/60Hz, Hot-plug redundant	
12.	Operating Conditions	0°C to 35°C or better	
13.	Form Factor	3U 1/2 19" Rack mount housing	
14.	Storage Temperature	0°C to 40°C	

6.8.4 PC – ICC

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Processor	Minimum Intel Core i7 processor @ 3.5 Ghz	
2.	RAM	32 GB	
3.	Internal storage	1 TB SATA 3.0Gb/s	
4.	Network Interface	2x10/100/1000	
5.	Graphics	NVIDIA® GeForce® GTX 1060 or equivalent	
6.	Display	3 Nos 24" LED screen Full HD	
7.	Keyboard & Mouse	USB based	
8.	Port	Minimum 4 Nos USB ports	

6.8.5 Printer

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Printers shall be of latest laser technology & for duplex printing (colour and black and white) for all paper size including but not limited to A4, A3 size.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	Technical	It shall have Print Speed 30ppm or above.	
3.	Technical	It shall have Resolution Min 600 X 600 dpi or better.	
4.	Technical	It shall have Memory 1 GB or higher.	
5.	Technical	It shall have Copy speed 12ppm or better.	
6.	General	It shall have scanner of Flat Bed type with ADF.	
7.	Technical	It shall have Interface USB 2.0, Ethernet Port.	
8.	General	It shall have the duty cycle of monthly 5000 pages at minimum.	
9.	General	Full toner Cartridge shall be supplied with the printer.	
10.	General	It shall have input tray capacity of minimum 100 sheets.	
11.	General	It shall have output tray capacity of minimum 100 sheets.	
12.	General	Printer shall be accompanied with the necessary accessories such as connecting cables, driver media, etc.	

6.8.6 Projector

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	3D Capable: Yes	
2.	General	Analog Video Signal: RGB, component video	
3.	General	Brightness:4000 lumens	
4.	General	Colour Support:1.07 billion colours	
5.	General	Contrast Ratio: 2200:1 / 10000:1 (dynamic)	
6.	General	Device Type: Projector with High Definition 720p or better display	
7.	General	Features:2x colour wheel	
8.	General	Interfaces:1 X VGA input - 15 pin HD D-Sub (HD-15)	
9.	General	Lamp Life Cycle: Up to 3000 hour(s) / up to 5000 hour(s) (economic mode)	
10.	General	Lamp Type:260 Watt	
11.	General	Lens Aperture: F/2.4-2.66	
12.	General	Min Operating Temperature:41 °F	
13.	General	Max Operating Temperature:104 °F	
14.	Projector	Native Aspect Ratio:0.67361	
15.	Projector	Output Power / Channel:10 Watt	
16.	Projector	Power: AC 230 V (50 Hz)	
17.	Projector	Projection Distance: 4 feet. - 33 feet.	
18.	Lens	Resolution: WXGA (1280 X 800)	
19.	Lens	Security Features: Security lock slot	
20.	Lens	Sound Emission:37 dB	
21.	Video Input	Sound Emission (Economic Mode):32 dB	
22.	Video Input	Sound Output Mode: Mono	
23.	Video Input	Speakers: Speaker(s) - integrated	
24.	Speakers	Speakers:1 X mixed channel	
25.	Speakers	Throw Ratio:1.28 - 1.536:1	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
26.	Speakers	TV System: PAL-B/G, PAL-N, PAL-M, PAL-I, NTSC 4.43, NTSC 3.58, PAL-D, SECAM L, PAL-H, SECAM K1, SECAM D/K, SECAM B/G	
27.	Speakers	Type: Integrated	
28.	Expansion / Connectivity	Uniformity:0.8	
29.	Miscellaneous	Video Input: RGB, component video (PAL-B/G, PAL-N, PAL-M, PAL-I, NTSC 4.43, NTSC 3.58, PAL-D, SECAM L, PAL-H, SECAM K1, SECAM D/K, SECAM B/G)	
30.	Environmental Parameters	Video Interfaces: VGA, HDMI	
31.	Environmental Parameters	Video Modes:480p, 720p, 1080i, 1080p, 480i, 576i, 576p	
32.	Environmental Parameters	Zoom Factor:1.2x	
33.	Environmental Parameters	Zoom Type: Manual	

6.8.7 PC – DC & Help desk

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Processor	Intel Core i7 processor @ 3.5 Ghz	
2.	RAM	32 GB	
3.	Internal storage	1 TB SATA 3.0Gb/s	
4.	Network Interface	2x10/100/1000	
5.	Graphics	NVIDIA ® GeForce ® GTX 1060 or equivalent	
6.	Display	3 Nos 21" LED screen Full HD	
7.	Keyboard & Mouse	USB based	
8.	Port	Minimum 4 Nos USB ports	
9.	Operating System	Pre-loaded OS latest	

6.8.8 Desktop

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Processor	Intel Core i7, 64bit x86 Processor @ 3.2 GHz or more,4MB L3 cache, Memory support DDR3 or better specifications	
2.	Motherboard & Chipset	OEM Motherboard	
3.	Video	Integrated Graphic controller	
4.	Network	Integrated 10 / 100 / 1000 Gigabit Ethernet controller	
5.	Ports	<ul style="list-style-type: none"> 1 HDMI port (Preferable), 2x USB 2.0 and 2 X USB 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> (Preferable), 10 USB ports external - with minimum 4 ports USB Front I / O includes (2 or more) USB 2.0 ports Rear I / O includes (2 or more) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS2 mouse and keyboard ports, RJ-45 network interface, Display Port 1 VGA and 3.5mm audio in /out jacks; 4 in 1 Media Card Reader (Preferable) 	
6.	HDD Controller	Integrated dual port SATA-II controller	
7.	Memory	8GB DDR III 1333MHz or higher expandable up to 16 GB or more	
8.	Storage	1TB @ HDD 7200 RPM	
9.	Optical Drive	22X DVD writer or higher and the corresponding software	
10.	Monitor	21" TFT LCD touch screen monitor minimum 1920 X 1080 resolution with 5 ms response time or better specifications, TCO 03 or higher certified	
11.	Keyboard	107 or more English + Punjabi and Rupee Symbol Keys keyboard	
12.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 cpi, Complying to CE and FCC norms	
13.	Power Management and DMI	System with Power management features & Desktop Management Interface implementation	
14.	Operating System	Supported by Windows, Linux etc.	
15.	Power input	100 -240V AC	
16.	Certifications	EPEAT	
17.	Graphic Card	Extra Graphic card for support Visuals	

6.8.9 IP Dome Camera for DC Surveillance

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General Requirements	The camera should be manufacturer's official product line designed for commercial / industrial 24x7x365 use. The camera and camera firmware should be designed and developed by same OEM	
2.	Image Sensor with WDR	1/3.2" with True WDR, Progressive CMOS Sensor or better	
3.	Lens Specs	Compatible to image sensor, Focal length 8-50 mm or better, Full HD (1080P), Auto IRIS / P IRIS, Corrected IR, CS Mount with IR cut filter	
4.	Resolution	Active Pixels 1920(w) X 1080(h)	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Minimum illumination	Colour: 0.3 lux or better, B/W: 0.05 lux or better	
6.	Video Encoder	H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG	
7.	Frame Rate	Shall support up to 30 fps	
8.	Local Storage	32 GB SD Card or higher	
9.	Ethernet	10/100/ Base-T ports	
10.	Protocols	Minimum of the following protocols to be supported RTSP, RTP/TCP, RTP/UDP, HTTP, HTTPS, DHCP	
11.	Industry Standards	ONVIF Compliant	
12.	Power Supply	POE IEE 802.3af compliant	
13.	Operating Temperature	0° C to 50° C or better	
14.	Operating Humidity	0% to 90% for cameras	
15.	Enclosure / Casing	IP 66	
16.	Certifications	UL, CE, C83FCC, ONVIF 2.X/S	
17.	Support	The system should not be an end of life / end of service product.	
18.	Streaming	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently.	
19.	White Balance	Auto / Manual	
20.	Back Light Compensation	Auto	
21.	Security	Security Password protection	
22.	Security	Vandal and impact resistant housing, IK 10, IP66, NEMA 4X	
23.	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS	
24.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features	
25.	Mounting Accessories	For pole and surface mount with L/C Brackets	
26.	IR Illuminator	External / build-in IR Illuminator with minimum 50 meters. In case of external, "IR Illuminator" section to be referred	

6.8.10 TV with accessories, Setup box, DTH Connection

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Screen Size	54.6" to 55" Measured Diagonally	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
2.	Display Panel	LED	
3.	Screen Resolution	1,920 (W) X 1,080 (H)	
4.	Aspect Ratio	16:09	
5.	Stand	Yes	
6.	Picture Mode	Dynamic/Normal/Cinema/Custom/Professional	
7.	Viewing Angle	178 degrees	
8.	Colour Space	Advanced Colour Spectrum	
9.	Noise Reduction	Multi-Noise Reduction	
10.	Media Player	Picture/Movie/Music	
11.	Support Format	AVCHD 3D/Progressive, SD-VIDEO/AVI/MKV/WMV/MP4/M4v/FLV/3GPP/VRO/VOB/TS/PS, MP3/AAC/WMA Pro/FLAC/WAV, JPEG/MPO	
12.	Sound Effect	Normal / Surround Sound	
13.	Sound Output (RMS)	10W X 2 Minimum	
14.	Speaker Type	Bottom / Side / Front / Back	
15.	Tuner	Digital: DVB-T 7MHz VHF / UHF; Analogue PAL B/G 7MHz VHF / UHF	
16.	Wi-Fi	Optional	
17.	Color Enhancer	Yes	
18.	Auto Power Off	Yes	
19.	Clock & On/Off Timer	Yes	
20.	HDMI	3	
21.	USB	2	
22.	Ethernet LAN	1	
23.	Component	1	
24.	Composite In (AV)	1	
25.	RF In (Terrestrial/Cable Input)	1	
26.	PC Audio Input (Mini Jack)	1	
27.	PC/DVI Audio In (Mini Jack)	1	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
28.	Digital Audio Out (Optical)	1	
29.	Audio Out (Mini Jack)	1	
30.	Optical	1	
31.	Dimensions (W X H X D) (w/o stand)	1,240 X 721 X 55 mm approx.	
32.	Dimensions (W X H X D) (with stand)	1,242 X 760 X 240 mm approx.	
33.	Weight (w/o stand)	20.0 kg approx.	
34.	Weight (with stand)	22.0 kg approx.	
35.	Included Accessories	TV Remote, AA/AAA Battery	
36.	Power Supply	AC 220 - 240 V, 50/60 Hz	
37.	Rated Power Consumption	1.20 A	
38.	Standby Power Consumption	0.20 W	
39.	ENERGY STAR® Certified	Yes, Exceeds Standards	
40.	Digital Broadcasting	ATSC/Clear QAM	

6.9 Non - IT Hardware

6.9.1 Fire Alarm System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	System Description	<p>The Fire alarm system shall be an automatic 1 to n (e.g. 24) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.</p> <p>Detection shall be by means of automatic heat and smoke detectors located throughout the Data Centre</p>	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		(ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.	
2.	Design	The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply	
3.	Control and indicating component	All controls of the system shall be via the control panel only	
4.	Control and indicating component	All site-specific data shall be field programmable and stored in an integral EEPROM. The use of EPROM's requiring factory 'burning' and re-programming is not acceptable.	
5.	Control and indicating component	All internal components of the control panel shall be fully monitored.	
6.	Control and indicating component	The control panel shall be capable of supporting a multi device, multi zone 2-wire detection loop. Removal of 1 or more detection devices on the loop shall not render the remaining devices on the loop inoperable.	
7.	Control and indicating component	The system status shall be made available via panel mounted LEDs and a backlit 8-line X 40-character alphanumeric liquid crystal display.	
8.	Control and indicating component	All user primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2. Essential controls, such as Start / Stop sounders and Cancel fault buzzer, etc. will be clearly marked.	
9.	Control and indicating component	Cancel fault and display test functions shall be configurable to be accessed from level 1 or level 2.	
10.	Control and indicating component	All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
11.	Event logging	The control panel shall log a minimum of 700 events comprising of 100 event fire log and 200 event fault, disablement and historic logs, giving time, date, device reference and status of indication.	
12.	Event logging	Fire, fault and disablement events shall be logged as they occur. Visual and audible conformation shall be given on an array of LEDs, the Liquid Crystal Display and the internal supervisory buzzer.	
13.	Power	The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions. The system shall be capable of full re-charge within 24 hours following full system discharge. The performance of the power supply and batteries shall be monitored and alarm rose, should a fault be detected. The system shall protect the batteries from deep discharge.	
14.	Power	All terminations within the control panel with the exception of the 230V mains connection will be via removable terminal screw fixing points.	
15.	User functions	The control panel will have a programmable maintenance reminder to inform the user that maintenance of the system is required. This function shall provide the user with the option of a monthly, quarterly, annually or bi-annually reminder prompts. The maintenance reminder will be indicated on the control panel. This message shall be resettable by the user and will not require the intervention of specialist support. The control panel will provide programmable free text field as part of the maintenance reminder facility.	
16.	User functions	The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
17.	Manual Controls	<ul style="list-style-type: none"> • Start sounders • Silence sounders • Reset system • Cancel fault buzzer • Display test • Delay sounder operation • Verify fire condition • Enter or modify device text label • Setup maintenance reminder • Assign or modify zones • Disable zones, device, sounders, FRE contact, auxiliary contacts • Enable zones, device, sounders, FRE contact, auxiliary contacts • Action weekly test • Disable loop 	
18.	Cable entries	The control panel will include the necessary top entry and rear entry cable entry points via 20mm knockouts.	
19.	Manual call points (MCP)	<ul style="list-style-type: none"> • MCP's shall be addressable and of the steady pressure break glass type manufactured to the requirements of BS 5839: Part 2. A test key shall be provided to allow the routine testing of the unit to meet the requirements of BS 5839 Part 1 1988, without the need for special tools or the need to unfasten the cover plate. • The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. The device shall incorporate a short circuit isolation device and a red LED indicator. • The MCP shall be suitable for surface or flush mounting. When flush mounted the device shall be capable of fixing to an industry standard single gang box. 	
20.	Smoke detectors	Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		indicate the device has operated and shall fit a common addressable base	
21.	Heat detectors	<ul style="list-style-type: none"> • Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point. • Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved. • The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base. 	
22.	Addressable detector bases	<ul style="list-style-type: none"> • All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator. • The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches. • Detector bases shall fit onto an industry standard conduit box. 	
23.	Audible Alarms	Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.	
24.	Commissioning	<ul style="list-style-type: none"> • The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel. • The labelling of Device and Zone labels should be part of the system. • Necessary Software to the control panel 	

6.9.2 Fire Suppression Systems

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design	The Clean Agent Fire Suppression system cylinder, Chief Controller of Explosives, Nagpur approved seamless cylinders, discharge hose, fire detectors and panels and all other accessories required to provide a complete operational system meeting applicable requirements of NFPA 2001 Clean Agent Fire Extinguishing Systems, NFPA 70 National Electric Code, NFPA 72 National Fire Alarm Code or ISO standards must be considered to ensure proper performance as a system with UL/FM approvals and installed in compliance with all applicable requirements of the local codes and standards.	
2.	Design	The Clean Agent system considered for Total flooding application shall be in compliance with the provisions of Kyoto Protocol.	
3.	Design	Care should be taken that none of the Greenhouse Gases identified in the Kyoto Protocol is used for fire suppression application	
4.	Design	The minimum criterion for the selection of the Clean Agent will be on the following parameters <ul style="list-style-type: none"> • Zero Ozone Depleting Potential. • Global Warming Potential not exceeding one. • Atmospheric Lifetime not exceeding one week. The clean agent fire suppression system with FK-5-1-12 and Inert Gas based systems are accepted as a replacement of HCFC and HFC as per Kyoto Protocol	
5.	Design	The Clean Agent considered for the suppression system must be suitable for manable occupied areas with NOAEL Level (No observable adverse effect level) of 10% as compared to the design concentration to ensure high safety margin for the human who might be present in the hazard area.	
6.	Design	The minimum design standards shall be as per NFPA 2001, 2004 edition or latest revisions.	
7.	Design	Care shall be given to ensure proper early warning detection system with minimum sensitivity of 0.03% per foot obscuration as per NFPA 318 & NFPA 72 to ensure that one gets a very early warning to investigate the incipient fire much before the other detectors activate the fire suppression system automatically.	
8.	Design	Additionally, Portable Extinguishers (CO2 or Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the Data Centre.	
OR			

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Design	Fire suppression system shall deploy FM-200 (ETG-5) based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.	
10.	Design	Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm	
11.	Compliance	The OEM (/ Bidder) shall give a Certificate stating that their FM-200 system is approved by UL / FM / VdS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).	
12.	Compliance	The OEM (/ Bidder) shall also provide a Letter that the OEM has FM-200 Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill of materials and that such Software shall be type approved by FM / UL / VdS / LPC.	
13.	Compliance	The Storage Container offered shall be of Seamless type, meant for exclusive use in FM- 200 systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.	
14.	Compliance	The Seamless storage cylinder shall be approved by Chief Controller of Explosives, Nagpur and shall have NOC from CCoE, Nagpur for import of the same. Documentary evidence to be provided for earlier imports done by the bidder.	
15.	Operating principle	The FM-200 valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.	
16.	Operating principle	The FM-200 Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally tested for periodic servicing requirements and without any need to replace consumable parts.	
17.	Operating principle	The individual FM-200 Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.	
18.	Operating principle	The system flow calculation be carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VdS / LPC/ UL / FM.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
19.	Operating principle	The system shall utilize 42 Bar / High pressure (600 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and allow for better agent penetration in enclosed electronic equipment such as Server Racks/ Electrical Panels etc.	
20.	Operating principle	The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the FM-200 system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.	
21.	Operating principle	The suppression system shall provide for high-speed release of FM-200 based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 7% (v/v) of FM-200 for 21 degrees Celsius or higher as recommended by the manufacturer.	
22.	General	The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.	
23.	General	Sub floor and the ceiling void to be included in the protected volume.	
24.	General	The FM-200 systems to be supplied by the bidder must satisfy the various and all requirements of the Authority having Jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.	
25.	General	The detection and control system that shall be used to trigger the FM-200 suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.	
26.	General	The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VdS / LPC.	
27.	General	The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the FM-200 containers.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
28.	General	FM-200 shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.	
29.	General	The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.	
30.	General	The FM-200 discharge shall be activated by an output directly from the 'FM-200' Gas Release control panel, which will activate the solenoid valve. FM-200 agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 600 psi (g) at 21°C with dry Nitrogen.	
31.	General	The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.	
32.	General	Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the FM-200 agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.	
33.	General	The manual release device fitted on the FM-200 Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, FM-200 cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.	
34.	General	FM-200 storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.	
35.	General	FM-200 containers shall be equipped with a pressure gauge to display internal pressure.	
36.	General	Brass Discharge nozzles shall be used to disperse the 'FM-200'. The nozzles shall be brass with female threads and available in sizes as advised by the OEM system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.	
37.	General	All the Major components of the FM-200 system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
38.	General	Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.	
39.	General	Release of FM-200 agent shall be accomplished by an electrical output from the FM- 200 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.	

6.9.3 ICCC facility Public Address System and Common Alarm System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<p>The PA system is required for:</p> <ul style="list-style-type: none"> • Making public announcement from the Security Control Room and Facility Manager's room. Clear and crisp announcement should reach to the entire Facility area. • Microphones should be provided to make announcements / respond to announcement from the designated location within the Facility. • To play light music if required. 	
2.	General	<p>Common Alarm System:</p> <ul style="list-style-type: none"> • The common alarm panel is required for checking the healthiness of all systems, to be installed at Data centre. • The panel can be installed in the room of Security Officer at Data centre. • The common alarm panel should have provision for accepting "potential free" signals from all system for relevant status change in that system 	

6.9.4 Humidity, Ventilation and Precision Air Conditioning Systems

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design Principle	<ul style="list-style-type: none"> • The Data Centre should be precision environment controlled. The temperature inside Server Farm area should be maintained at 20 degree centigrade with a precision of ± 1 degrees. • The Precision Air Conditioning shall be provided for the Server Farm with around 370 sq.ft. area with necessary enhancements of cooling capacity 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<p>in future in terms of additional indoor and outdoor units.</p> <ul style="list-style-type: none"> The bidder should plan the location of such additional indoor and outdoor units. Bidder should also plan the location of such additional units in the area and lay additional conduits (including associated civil / electrical works) between locations of these additional indoor units and outdoor units, lay additional electrical cable & outlets so as to have other infrastructure ready for deploying additional indoor and outdoor units at a future date. <p>Air Conditioning should be ensured to the extent of 99.9%. It is suggested to provide air supply typically through false flooring</p>	
2.	Air Conditioning	<p>The HVAC system shall provide the cooling for the following Zones:</p> <p>Zone A: Server Farm Area Zone B: ICCR Room, NOC, BMS, UPS Room, Telecom Room, Staging Room Zone C: War Room</p> <p>Since Zone A is a critical area, a separate air conditioning system (precision air conditioning) should be exclusively installed to maintain the required temperature for Zone A (Server Farm). Zone B & C can have a common air conditioning system for comfort. The general requirements for the two zones are as specified below:</p> <ul style="list-style-type: none"> Zone A – should be provided with precision air conditioning on a 24 X 7 X 365 days operating basis at least meeting with Tier – III having n + 1 redundancy architecture requirements and having enough provision to scale it to next level as may be required in a later stage. The units should be able to switch the air conditioner on and off automatically and alternately for effective usage in pre-defined sequence. The units should be down-flow fashion, air-cooled conditioning system. Precision Air Conditioning 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<p>systems specifically designed for stringent environmental Control with automatic monitoring and control of cooling, heating, humidification, dehumidification and air filtration function should be installed.</p> <ul style="list-style-type: none"> Zone B should be provided with Centralized Cooling System for Comfort System <p>Zone C should be provided with split-type comfort air-conditioning system</p>	
3.	Ducting Requirements	It is Ideal for higher power system the gap between false floor and true floor should be used to deliver conditioned air to the desired space, the Floor Discharge System to eliminate the requirement of duct. This can be taken care as and when such system comes to DC to such needs. However, proper ducting mechanisms should be ensured for the requirement of Air Conditioning	
4.	Natural Convection	As the conditioned air is supplied through the grills with volume control dampers on the floor, the cold air-cools the component in a much faster and efficient manner as it does moves up, after extracting heat from the component. This follows the natural convection path of the air. The warm air should be sucked at the top by machine, air-conditioned and then supplied back to the room.	
5.	Air Distribution	The air is to be distributed evenly by providing grills with VCDs (Volume Control Dampers) in the floor tiles.	
6.	Flexibility	The system should give the flexibility of discharging air at wherever point required even if the furniture is relocated. Changing the grill/tiles carrying grills, at suitable location does this.	
7.	General	The precision air-conditioners should be capable of maintaining a temperature range of 20 degree with a maximum of 1-degree variation on higher and lower side and relative humidity of 50% with a maximum variation of 5% on higher and lower side.	
8.	General	The precision air-conditioners shall have 2 independent refrigeration circuits (each comprising 1 no scroll compressors, refrigeration circuit and condensers) and dual blowers for flexibility of operations and better redundancy.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	General	The unit casing shall be in double skin construction for longer life of the unit and low noise level.	
10.	General	For close control of the DC environment conditions (Temp. and RH) the controller shall have (PID) proportional integration and differential.	
11.	General	The precision unit shall be air cooled refrigerant based system to avoid chilled water in critical space.	
12.	General	The internal rack layout design shall follow cold aisle and hot aisle concept as recommended by Ashrae.	
13.	General	The refrigerant used shall be environment friendly HFC, R-407-C/ equivalent in view of long term usage of the data Centre equipment, availability of spares and refrigerant.	
14.	General	Thermal and CFD Analysis diagrams should be provided	
15.	General	The fan section shall be designed for an external static pressure of 25 Pa. The fans shall be located downstream of the evaporator coil and be of the electronically commuted backward curved centrifugal type, double width, double inlet and statically and dynamically balanced. Each fan shall be direct driven by a high efficiency DC motor.	
16.	General	Dehumidification shall be achieved by either reducing effective coil area by solenoid valve arrangement or using Dew point method of control. Whenever dehumidification is required, the control system shall enable a solenoid valve to limit the exchange surface of the evaporating coil, thereby providing a lower evaporating temperature.	
17.	General	The humidifier and heaters shall be a built in feature in each machine individually. Humidification shall be provided by boiling water in a high temperature polypropylene steam generator. The steam shall be distributed evenly into the bypass airstreams of the environment control system to ensure full integration of the water vapour into the supply air without condensation. The humidifier shall have an efficiency of not less the 1.3 kg/kw and be fitted with an auto flush cycle activated on demand from the microprocessor control system. The humidifier shall be fully serviceable with replacement electrodes. Wastewater shall be flushed from the humidifier by	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		the initiation of the water supply solenoid water valve via a U-pipe overflow system. Drain solenoid valves shall not be used. Microprocessor should be able to control the humidification and heating through suitable sensor	
18.	Status display	<ul style="list-style-type: none"> • Room temperature and humidity. • Supply fan working status • Compressor working status • Condenser fans working status • Electric heaters working status • Humidifier working status • Manual / Auto unit status • Line voltage value • Temperature set point • Humidity set point • Working hours of main component i.e. compressors, fans, heater, humidifier etc. • Unit working hours • Current date and time • Type of alarm (with automatic reset or block) <p>The last 10 intervened alarms</p>	
19.	Microprocessor controlled functions	<ul style="list-style-type: none"> • Testing of the working of display system • Password for unit calibration values modification • Automatic re-start of program • Cooling capacity control • Compressor starting timer • Humidifier capacity limitation • Date and time of last 10 intervened alarm • Start / Stop status storage • Random starting of the unit. • Outlet for the connection to remote system • Temperature and humidity set point calibration • Delay of General Alarm activation • Alarm calibration 	
20.	Alarms	<ul style="list-style-type: none"> • Air flow loss • Clogged Filters • Compressor low pressure • Compressor high pressure • Smoke - fire 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> • Humidifier Low water level • High / Low room temperature • High/Low room humidity • Spare External Alarms • Water Under floor 	
21.	User Settings	<ul style="list-style-type: none"> • Unit identification number • Start-up Delay, Cold start Delay and Fan Run on timers • Sensor Calibration • Remote shutdown & general Alarm management • Compressor Sequencing • Return temperature control • Choice of Modulating output types 	
22.	Protection	<ul style="list-style-type: none"> • Single phasing preventers • Reverse phasing • Phase imbalancing • Phase failure • Overload tripping (MPCB) of all components 	
23.	Air quality levels	<p>The DC shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The DC shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, blocking the function of moving parts, causing components to overheat etc. Air filters shall be 95% efficiency & provide up-to 5 Micron particulate shall be deployed</p>	
24.	Relative Humidity	<p>Relative Humidity (RH) requirements Ambient RH levels shall need to be maintained at 50% ± 5 non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24x7 basis and logged for providing reports.</p>	

6.9.5 Water Leakage Detection System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The water leak detector shall be installed to detect any seepage of water into the critical area and alert the Security Control Room for such leakage. It shall consist of water leak detection cable and an alarm module. The cable shall be installed in the ceiling & floor areas around the periphery.	
2.	Design	Water Leak Detection system should be for the Server and Network room Areas to detect and water flooding below the floor of the DC.	
		Water Leak Detection System should be wire based solution with alarm; the wire needs to lay in DC surrounding the PAC units, which is the probable source of water leakage.	

6.9.6 Rodent Repellent System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design	The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However, periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.	
2.	Configuration	Master console with necessary transducer	
3.	Operating Frequency	Above 20 KHz (Variable)	
4.	Sound Output	50 dB to 110 dB (at 1 meter)	
5.	Power output	800 mW per transducer	
6.	Power consumption	15 W approximately	
7.	Power Supply	230 V AC 50 Hz	
8.	Mounting	Wall / Table Mounting	

6.9.7 Split Type Air-conditioner 2 Ton for Comfort Cooling

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Capacity	2 Tonnage Inverter type BEE 4 star or above	
2.	Cooling Capacity	Minimum 25000 BTU / Hr	
3.	Compressor	Hermetically Sealed Scroll Type	
4.	Refrigerant	R410 Type	
5.	Noise Level	< 50 dB	
6.	Operation	Wireless Remote Control	

6.9.8 Lighting

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	All overhead lighting shall be LEDs both recessed direct and indirect lighting, including pot-lights.	
2.	General	The overhead lighting treatment shall be incorporated into the other ceiling elements to create an aesthetic specialty ceiling design, in combination with the Rooms.	
3.	Technical	Overhead lighting intensity shall be: <ul style="list-style-type: none"> • For Command & Control Centre: at least 400 lux • For Network Operation Centre: at least 400 lux • For War Room: at least 500 lux • For Server Farm Area: at least 500 lux • UPS Room: at least 500 lux • BMS Room: at least 500 lux 	
4.	Technical	Dimming control shall be continuous (all lights dimmable) and zone-based (with a minimum of 4 lighting zones on separate circuits).	
5.	Technical	Dimming control shall have various configurations pre-set for the ideal operations lighting environment, based on the perimeter glass wall natural lighting conditions (e.g., sunny, cloudy, partly cloudy, night, etc.)	
6.	General	Appropriate wall boxes for corresponding dimmer size shall be provided.	
7.	General	Dimmers shall not be ganged in one box.	
8.	General	Manual switches shall be used for on / off lighting control and for overriding any pre-set lighting configurations.	
9.	General	Cover plates for switches shall match the colour of switches, receptacles, and receptacle cover plates. Cover plates shall be of the same manufacturer as the devices.	
10.	General	All lighting fixtures shall be of high-grade quality over and above the standard level of quality for office lighting.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
11.	General	Lighting arrangement shall accommodate console locations.	
12.	General	Lighting shall be configured in order to reduce glares and reflections on console monitors and on the video wall, as well as accommodate any other lighting needs the monitors and video wall may have.	

6.9.9 Diesel Generator

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design	Water cooled, Naturally Aspirated 1500 RPM. under NTP conditions of BS: 5514, with Dry Type Air Cleaner, Compact Radiator with Recovery Bottle and Pusher type Fan, Engine with Coolant, Engine mounted panel with wiring harness, Holset Coupling and Industrial Silencer, as per engine manufacturers design standards. Power output guaranteed within 0 to +2 % and can be operated up to 3130 Mt. altitude and no de-rating for ambient temperature or humidity. The DG units should come with sound proofing as per the standards	
2.	Alternator	Standard design Alternator, rated at 0.8 PF, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec	
3.	Alternator	1500 RPM, self-excited and self-regulated, with brushless excitation	
4.	Alternator	Self- ventilated, Screen Protected Drip Proof,	
5.	Alternator	Insulation Class "H",	
6.	Alternator	enclosure IP 23	
7.	Alternator	The A.C. Generator shall be Horizontal foot mounted single bearing type and shall be fitted with Automatic Voltage Regulator (AVR) for Voltage regulation of +/- 1% or better. The Alternator generally conforms to BS: 5000/IS: 4722 and suitable to deliver output of suitable engine capacity	
8.	Base Frame	Sturdy, fabricated, welded construction, channel iron Base Frame for mounting the above Engine and Alternator	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Control Panel	Cubicle type, floor mounting Control Panel, with hinged doors, bottom gland plate and accommodating the following: <ul style="list-style-type: none"> ○ 1-No. ACB or Moulded Case Circuit Breaker ○ 3-No.'s Ammeters /1 No. Ammeter with Selector Switch ○ 1 No. Voltmeter with Selector Switch ○ 1 No. frequency meter ○ 1 Set Pilot Lamps LOAD ON/GENERATOR ON ○ 1 Set Instrument Fuses 	
10.	Fuel Tank	Necessary litters capacity Fuel Tank with mounting brackets to run for 8 hours, 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. Diesel storage requirement for minimum 72 hours should be maintained	
11.	Battery	Dry uncharged maintenance free batteries with leads and terminals	
12.	Management	The DG set should be manageable via Building Management System/ NOC with MODBUS Protocol with RS 485 Communication Port so that all software features like Diesel Consumption, Power, and Current etc. can be monitored on the BMS screen	

6.9.10 Online UPS 60 KVA and 20 KVA

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	UPS Load distribution	UPS A- 60 KVA for Server Racks and Video Wall UPS B- 20 KVA for IT equipment (Workstations/ PCs,) and Lights, one TV, printer and IP Phones	
2.	Input Range	Input Standard Voltage, 380 /400 / 415 V 3 Phase, 3 or 4 wire, +10 %, -15%	
3.	Output Voltage & Waveform	Input Frequency, 50 Hz, +5% or -5%	
		Output Steady State Voltage, 380 / 400 / 415 V +1% or -1%	
4.	Battery Backup	30 mins on each UPS	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
5.	Output Frequency	Output Frequency, 50 Hz, +0.25Hz to 0.5Hz	
6.	Voltage	Output Transient Voltage Stability, < 5% or –5% for a load change from 0% to 100%	
7.	Voltage	Overload – 125% for 10 minutes and 150% for 60 seconds	
8.	Efficiency	Efficiency at full rated load, Not less than 92%	
9.	Harmonic	Total Harmonic Content – With Linear Load < 2% for 100 % linear load and with 3:1 Crest factor load < 5%	
10.	Harmonic	Input Harmonic Filter (for <10% Input current distortion)	
11.	DC ripple	DC ripple (with & without Battery connected) < 1%	
12.	General	Built In power factor correction	
13.	General	Automatic shutdown of component for longer power outages	
14.	General	Monitoring and logging the status of the power supply	
15.	General	Displaying the voltage/current draw of the component	
16.	General	Automatic restarting of component following a power outage	
17.	General	Displaying the current voltage on the line	
18.	General	Providing alarms on some error connections	
19.	General	Providing protection against short circuits	
20.	Temperature Range	Operating Temperature range - 0 to 40 Celsius, Maximum 50 Celsius for 8 hrs	
21.	Design	Design compliance with IEC and ISO	
22.	Design	Software that must be installed and integrated suitable operating system	
23.	Design	Supplies True Online UPS Power	
24.	Design	Non-Linear load compatible	
25.	Design	Capability to handle high Crest Factor load	
26.	Design	Ventilation- Air cooling with Integral Fans	
27.	Design	Built in Reliability & High Efficiency	
28.	Design	Low Audible Noise	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
29.	Design	Compact Footprint	
30.	Design	Front Access for easy Maintenance	
31.	Design	The power factor of the UPS system shall be at 0.90 or above at all load conditions	
32.	Design	Input Current Harmonics < 10%	
33.	Design	The battery circuit breaker MCCB shall have O/L and U/V protection.	
34.	Design	The UPS shall have built in isolation transformer for re-referencing and to limit neutral- ground voltage to 1.50 volts by directly connecting dedicated earth to neutral of the output isolation transformer of the UPS as stipulated by server manufactures	

6.9.11 Access Control

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Design requirement	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 Proximity as well as Biometric Technology and Password for the critical areas and Proximity technology for non-critical areas	
2.	Design requirement	An access control system consisting of a central PC, intelligent controllers, proximity readers, power supplies, proximity cards and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for doors	
3.	Design requirement	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	
4.	Monitoring	The system shall monitor the status of the doors through magnetic reed contacts	
5.	Access Control	Controlled Entries to defined access points	
6.	Access Control	Controlled exits from defined access points	
7.	Access Control	Controlled entries and exits for visitors	
8.	Manageability	Configurable system for user defined access policy for each access point	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Manageability	Record, report and archive each and every activity (permission granted and / or rejected) for each access point.	
10.	Manageability	User defined reporting and log formats	
11.	Manageability	Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.	
12.	Manageability	Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.	
13.	Manageability	One user can have different policy / access rights for different access points	

6.10 Helpdesk Hardware

6.10.1 IP phone

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
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/H.323	
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	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
14.	Ringer	Selectable Ringer tone	
15.	Directory Access	LDAP standard directory	
16.	QoS	QoS mechanism through 802.1p/q	

6.10.2 IP PBX and Voice Router

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The IP telephony system should be a converged communication System with ability to run analog and IP on the same platform using same software load based on server and Gateway architecture	
2.	Scalability	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	
3.	General	The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted	
4.	Architecture	The voice network architecture and call control functionality should be based on SIP/H.323	
5.	Redundancy	The call control and system management should support redundancy with no single point of failure	
6.	IP Support	The communication server and gateway should support IP V6 from day one so as to be future proof	
7.	General	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM	
8.	General	Support for call-processing and call-control	
9.	Protocols	Should support signaling standards/Protocols– SIP, MGCP/ H.323, Q.Sig	
10.	Codecs	Voice Codec support - G.711, G.729, G.729ab, g.722	
11.	GUI	The System should have GUI support web based management console	
12.	Security	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS	
13.	Security	System should support MLPP feature	
14.	Security	Proposed system should support SRTP for media encryption and signaling encryption by TLS	
15.	Security	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	
16.	Security	The administrator logging on to the call control server needs to authenticate by suitable mechanism	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		such as User Login Information and Passwords/ Radius Server	
17.	General	Voice gateway to be provided with 1 PRI card with 2 port scalable to 3 PRI in future for PSTN (PRI) line termination.	

6.10.3 IVR & ACD

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	High Availability	Should support high availability with hot standby server that should provide seamless failover in case of main server failure. There should not be any downtime of Contact Centre in case of single server failure in high availability case	
2.	Routing	Should support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups	
3.	Routing	ACD support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialled number etc.	
4.	Routing	ACD should support call routing based on longest available agent, circular agent selection algorithms.	
5.	Queuing	ACD should 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/ expected delay.	
6.	Chat	Agents should be able to chat with other Agents or supervisor and solution shall be provided with minimum 10 Agent licenses	
7.	Status	Supervisor should be able to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop	
8.	Queuing	Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.	
9.	Active/Standby Mode	In future if required, the ACD should support active and standby server mode, where the server can be put in DC and DR. ACD solution should support placing of Main and Stand by server in DC and DR respectively.	
10.	DTMF	IVR should play welcome messages to callers Prompts to press and collect DTMF digits	
11.	GUI	GUI based tool to be provided for designing the IVR and ACD call flow.	
12.	Call Flows	IVR should support Voice XML for ASR, TTS, and DTMF call flows	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
13.	Read Capability	IVR should be able to Read data from HTTP and XML Pages	
14.	Campaigns	IVR should be able to run outbound campaigns.	
15.	Performance Analysis	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.	
16.	Performance Analysis	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes	
17.	Performance Analysis	Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit or SQL stored procedures.	
18.	Performance Analysis	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/CSV.	
19.	Email	Administrator should be able to assign one or more email addresses to a single Queue.	
20.	Email	Email routing support integration with Microsoft Exchange 2003 or Microsoft Exchange e2007 or 2010.	
21.	Email	Agents should be able to automatically resume of e-mail processing on voice disconnect.	
22.	Email	Agent should be able to save email draft response and resume at a later time.	
23.	Email	Agent should be able to re-queue email.	
24.	Email	Supervisor should be able to access real-time reporting for Agent E-Mail by mail volume	

7 Annexure III: Technical Specifications Software

7.1 Data Centre Platform Software

7.1.1 Integrated Command Control Centre (ICCC) Platform

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Data Normalization capabilities	<ul style="list-style-type: none"> It is envisaged that the city shall implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are Smart Traffic, Smart Parking, Smart Lighting, Energy Metering, Water Metering, CCTV, Public Transport and other integrations as per defined scope. The platform shall also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration. The platform shall be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers. The platform shall support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control. 	
2.	GIS Map Support	System shall support ESRI, Map Box, Open street etc. GIS and Map Servers	
3.	Location engine	<ul style="list-style-type: none"> Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities. Geospatial calculation: calculates distance between two or more locations on the map. 	
4.	Device engine	<ul style="list-style-type: none"> Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud. Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine. 	
5.	Data and Analytics engine	Data archive and logging: stores data feeds from the device engine and external data sources. Analytics: provides time-shifted or offline analytics on the archived data.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
6.	Data and Analytics engine	Reporting: delivers reports based on events triggered by device engine data and external notifications.	
7.	Developer Program tools	Sensor platform OEM shall provide online Developer Program tools that shall help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost.	
8.	Authentication, Authorization	System shall support standard Authentication, Authorization Performs.	
9.	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform.	
10.	API Repository / API Guide	<ul style="list-style-type: none"> Normalized APIs shall be available for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example, Lighting APIs: Vendor agnostic APIs to control Lighting functionality. Platform OEM shall have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform. Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future). 	
11.	Platform upgrade and maintenance	<ul style="list-style-type: none"> The OEM shall be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration. Platform shall be able to be deployed on a public cloud for disaster recovery. 	
12.	Platform functionality	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs.	
13.	Platform functionality	User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions.	
14.	Platform functionality	Application management: Provides role-based access view to applications.	
15.	Platform functionality	The platform shall also be able to bring in other e-governance data as i-frames in the command and control centre dashboard.	
16.	Platform functionality	All of these data shall be rendered / visualized on the command and control centre dashboard.	
17.	Integration capabilities	This platform is expected to integrate various urban services devices at the street layer so that urban	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		services applications can be developed on top of this platform independent of the technology that is used in the devices.	
18.	Integration capabilities	Integrate devices using their APIs in to this platform. For example, if the City wants to deploy Smart Parking solution, this platform shall have the ability and provision to write adaptors which interface with the parking sensors or management software of the parking sensors to collect parking events, data and alerts and notifications from the devices and their software managers.	
19.	General	The same logic and requirement applies to various other urban services devices like LED control nodes, water meters, energy meters, environmental sensors, waste bin sensors, device embedded in connected vehicles etc.	
20.	General	Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc.)	
21.	General	Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices.	
22.	General	Provides urban services API(s) to develop Operations applications for each of the Urban Services domains. For example, the lighting operator of the City shall be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application shall also have the ability to access data from other domains like environment based on the access control configured in the system.	
23.	Policies and Events	System shall allow policy creation to set of rules that control the behaviour of infrastructure items. Each policy shall a set of conditions that activate the behaviour it provides. System shall allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.	
24.	Policies and Events	System shall provision to define a set of conditions that can be used to trigger an event-based policy	
25.	Notifications, Alerts and Alarms	System shall generate Notification, Alert and Alarm messages that shall be visible within the Dashboard/GIS Platform and the Enforcement Officer Mobile App if required.	
26.	Notifications, Alerts and Alarms	All system messages (notifications, alerts and alarms) shall always be visible from the	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.	
27.	Notifications, Alerts and Alarms	Systems shall deliver message to a set of subscribers. The Notification service shall support min. two types of notification methods – Email notification and Short Messaging Service (SMS) notification.	
28.	Users and roles	Users access and perform 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 shall be associated with one or more roles and each role is assigned a certain set of permissions.	
29.	General	These roles and permissions define the tasks that a user can perform. Additionally, system shall assign one or more locations to each role so that the user can perform tasks at the assigned locations only.	
30.	General	Roles and permissions define the tasks that a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. Each user shall be associated with one or more roles and each role has an assigned set of permissions.	
31.	General	The platform shall allow different roles to be created and assign those roles to different access control policies.	
32.	General	System shall support LDAP to be used as an additional data store for user management and authentication.	
33.	Service Catalogue Management	The Service catalogue management module shall allow to categorize the externalized and non-externalized services into logical groups by creating the service catalogues. In addition, system shall allow manage the service catalogue by adding, modifying or deleting the catalogue details.	
34.	Reports	The platform shall have capability to provide access to real-time data and historical data from various connected devices for reporting and analytics.	
35.	Reports	System shall allow dashboard to generate reports and have provision to add reports in favourites list.	
36.	Data Security	The access to data shall be highly secure and efficient.	
37.	Data Security	Access to the platform API(s) shall be secured using API keys.	
38.	Data Security	Software shall support security standards: OAuth 2.0, HTTPS over SSL/TLS or equivalent security standards help protect the data across all domains.	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
39.	Global Market Presence & Support System	Smart city suppliers shall be adaptable to the emerging needs of cities. Suppliers shall develop offerings that meet the growing interest in urban Internet of Things (IoT) applications, big data solutions, and the transformation in city approaches to energy policy, urban mobility, and city resilience.	
40.	General	Smart City Platform/Software provider shall be global Member of Smart Cities Council & Navigant Research Report for Smart Cities Suppliers.	
41.	General	ICCC OEM shall have registered office in India at least from last 05 Years and shall have software development center in India. Shall have Quality Management System ISO 9001 OR Environmental Management System ISO 14001 Quality Certifications.	
42.	Standard Operating Procedure	Command & Control Centre shall provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.	
43.	Standard Operating Procedure	Standard Operating Procedures shall be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an Operations.	
44.	Standard Operating Procedure	The users shall be able to edit the SOP, including adding, editing, or deleting the activities.	
45.	Standard Operating Procedure	The users shall be able to also add comments to or stop the SOP (prior to completion).	
46.	Standard Operating Procedure	There shall be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.	
47.	Standard Operating Procedure	The SOP Tool shall have capability to define the following activity types:	
48.	General	Manual Activity - An activity that is done manually by the owner and provide details in the description field.	
49.	General	Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.	
50.	General	If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.	
51.	General	Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
52.	General	SOP Activity - An activity that launches another standard operating procedure.	
53.	Export Formats	System shall allow export the analysis into min following formats: a) XML/JSON b) Excel c) PDF d) CSV	
54.	Video Display and integration capabilities	a) Integrates with existing cameras and new cameras. Shall support multiple video sources from multiple locations. Platform shall have no limitation in displaying the number of CCTV video sources. b) Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence. c) Display module shall have capability to control multi-screened display wall in sync with operator console. d) Smart City Operations Centre shall support 20 to 30 camera feeds in display.	
55.	Technical support centre	ICCC OEM shall have 24 X 365 technical assistance support centre (TASC) in India. TASC shall provide online website and phone number to register service request, service request can be raise by partner and customer.	
56.	CCC Operations	a) The solution shall be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable. b) 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. c) The solution shall also provide an integrated user interface for all the smart elements implemented. d) The solution shall 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,	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<p>acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.</p> <p>e) The solution shall provide the “day to day Operations”, “Common Operating Picture” and situational awareness to the centre and participating agencies during these modes of Operations.</p> <p>f) It shall improve scalability for large and geographically distributed environments.</p> <p>g) It shall provide complete view of sensors, facilities, e-governance/ERP, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.</p> <p>h) It shall provide a uniform, coherent, user-friendly and standardized interface.</p> <p>i) It shall provide possibility to connect to workstations and accessible via web browser.</p> <p>j) The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.</p> <p>k) The solution shall allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes.</p> <p>l) The solution shall be available via a VPN as a web-based interface or a thin-client interface.</p> <p>m) It shall be possible to combine the different views onto a single screen or a multi-monitor workstation.</p> <p>n) The solution shall maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.</p> <p>o) The solution shall provide ability to extract data in desired formats for publishing and interfacing purposes.</p> <p>p) The solution shall provide ability to attach documents and other artefacts to incidents and other entities.</p> <p>q) The solution is required to issue, log, track, manage and report on all activities underway during these modes of Operations:</p>	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> • anticipation of incident • incident or crisis • recovery • incident simulation 	
57.	API & Interface Security	<p>a) The access to data shall be highly secure and efficient.</p> <p>b) Access to the platform API(s) shall be secured using API keys.</p> <p>c) Software shall support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.</p> <p>d) Shall 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.</p>	

7.1.2 Enterprise Content & Document Management System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<p>Facility to scan and upload</p> <ul style="list-style-type: none"> • Paper documents • Photos • Email communication • Any other document 	
2.	General	The system shall support all types of documents in electronic soft form (pdf, txt, xls, doc, ppt, picture files, TIFF, JPEG, GIF, even Zip Files etc.)	
3.	General	Ability to share documents scanned across several offices / departments.	
4.	General	System shall have support for management of image formats such as JPG, GIF, PNG, TIFF etc.; as well as output formats such as JPG, GIF and PNG etc.	
5.	General	System shall have support for video formats such as Flash (FLV), Real, Windows Media Format (WMV), QuickTime (MOV), MP4, AVI and others. Image and Video metadata is extracted and associated with the content item as object metadata.	
6.	General	Ability to support Web based scanning. It shall be possible to scan and upload documents including	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		pictures and images. Such document may be uploaded directly from third party premises over the web or from the office.	
7.	General	Ability to check the quality of the scanned image and make corrections/adjustments to improve the quality of the scanned image.	
8.	General	The ECM shall support temporarily storing the scanned images locally before uploading to the central server.	
9.	General	Ability to support quick scanning and indexing of bulk documents. Scanning through browser plug-in.	
10.	General	Ability to support automatic cropping / masking of whole/any part of the document. This ability should be user defined and document wise.	
11.	General	It shall be possible to set up and track both mandatory and non-mandatory documents.	
12.	General	Confirm that the content was delivered and viewed as a proof of compliance with security policies	
13.	General	Grant access to documents with feature of sharing file for a specified period of time while maintaining audit capabilities.	
14.	General	The system shall have a native iOS and Android based mobile/tablet app for easy access of the information (document) while users are on the move.	
15.	General	Create predefined linear routes for automatic document routing. This must be offered as a base and standard product	
16.	General	Facility of associating a note-sheet with the file enabling users to comment and review.	
17.	General	Facility of attaching documents and folders in work items	
18.	General	Time -based/ Event -based reminders	
19.	General	Provision of putting shared and secured notes for collaborative working on Work items	
20.	General	Ability to support typical document imaging annotations which include:	
21.	General	Highlighting images and text in various colours to emphasize words or sections	
22.	General	Redacting (blacking-out or whiting-out) images and text to preserve confidentiality	
23.	General	Stamping images with words such as FAXED or CONFIDENTIAL, or with signatures denoting approval or denial	
24.	General	Attaching sticky notes that contain additional comments	
25.	General	An imaging system 's security should control who can view	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
26.	General	<ul style="list-style-type: none"> Annotations such as highlighting, stamps or sticky notes, and who can see through redaction. All annotations should be overlaid and not change the actual image. Ability to support Printing, faxing and e-mailing documents 	
27.	General	System shall provide web-based administration tool and provide a single point of access for managing and administering all repositories, servers, users and groups regardless of their location across the enterprise	
28.	General	The system shall allow content syndication service via xml based feeds, email alerts etc.	
29.	General	The system shall support versioning of documents, user should be able to access previous and next versions with details like major and minor versions and the comments captured for the change.	
30.	General	Shall support storage of complete and multiple versions of content	
31.	General	Shall have major & minor release for draft & final release version of the document	
32.	General	Shall support the JSR 170, Java APIs/REST APIs/Web Service APIs that make content assets available to the application layer services or other Content Management (CM) solutions.	
33.	General	Shall support for storage of any type of contents such as JPG, TIFF, PDF, MS office files, audio, video, auto cad files etc.	
34.	General	The product shall support single metadata store for modules such as Document Management, Web Content Management, Records Management and Digital Asset Management	
35.	General	System should provide library services such as core content services, archiving, folders, content publishing, records management and security features.	
36.	General	Ability to support a single Security model for the content repository that is used to manage documents, records as well as web content.	
37.	General	System shall support for auditing for usage of content through audit trails	
38.	General	System shall provide support for scheduling indexing	
39.	General	Provides ability for administrators to archive and backup content	
40.	General	Shall support for both centralized & distributed architecture	
41.	General	Shall support for content cache for remote client	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
42.	General	Shall have policy-based, pluggable framework for reliability and secure access.	
43.	General	Shall have a comprehensive access control functions, depending on the user role & access levels	
44.	General	The proposed system shall be able to classify any piece of content as a record	
45.	General	Support for creation, declaration, classification, retention and destruction of business records.	
46.	General	System shall provide audit trails and certificate of destruction.	
47.	General	System shall provide the ability to freeze the records.	
48.	General	Product shall provide records managers with a single view into all retention schedules, disposition actions, and audit histories, facilitating the process of identifying and declaring records.	
49.	General	System shall allow for management of external content.	
50.	General	System shall support adapters to external repositories for managing records, such as file systems, content repositories and e-mail archives	
51.	General	Product shall provide generic adapters that can be configured for integration with other applications and repositories.	
52.	General	It shall have out of box components and integration options with Portal	
53.	General	The system shall provide ability to leverage multiple display templates for a content item	
54.	General	System shall support in-context web content contribution, preview, updates and approvals.	
55.	General	System shall provide support for multi-site management	
56.	General	The system shall provide spell-checking functionality. The language of the dictionary must be able to be changed for content authors producing content in other languages.	
57.	General	The system shall provide the ability to upload and associate media items to content items from within the content item authoring interface.	
58.	General	The system shall provide the ability to preview content as it shall appear on pages where it is added in production prior to it being published	
59.	General	Digital Certificate Services: The system should automatically enable/disable the Digital Signature Certificates (DSCs) of employees depending on the current status of each employee namely, fresh appointment / transfer / leave/ training / retirement etc. The system should accordingly	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		enable DSC only for an "active" employee. Procurement of digital certificates for the users of the ASCL shall be the responsibility of the client.	
60.	General	MAILING AND MESSAGING SERVICES: This would be used for sending the alerts as mail and SMS message to the registered users of the application and shall be used for messaging and calendaring services. The Mail and SMS Server should provide a highly available, scalable and reliable platform for delivering secure communication services. It would be required to cluster this Server to ensure high availability and reliability. This server shall also act as Messaging Server. It should provide with extensive security features ensuring the privacy of users and the integrity of communication through user authentication, session encryption, and content filtering to help prevent spam and viruses, and mechanisms to monitor and enable regulatory compliance. It should support standard SMTP, IMAP and POP3 services. The Messaging system should provide a secure messaging and collaboration – email solution with standard features like calendaring, contacts and tasks, Archiving, Directory and LDAP address book, web based access to emails and support for data storage. Other features to be supported include – per-user filtering policies, user management, mailing list manager and synchronization with MS Outlook / Lotus Notes/equivalent. Approximate size of mailbox for registered user should be 1 GB.	
61.	General	PAYMENT GATEWAY: The application would provide the online payment services through integration with the payment gateways. The solution shall support card payments using all the popular debit and credit cards (Visa, Master card etc.) and Direct Debit. For online payments, Secure Socket Layer (SSL) shall be used for supporting & securing the transactions taking place through the payment gateway. As Commercial transaction over internet is prone to Identity Theft and can cause financial loss to department and citizens, the solution would incorporate PCI DSS ver. 1.1 standards.	

7.1.3 Enterprise Management System (EMS)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise	
2.	General	The EMS shall be able to support the proposed hardware and software Components (IT and Non-IT) deployed. The software shall be capable of providing early warning signals on the performance issues, and future infrastructure capacity augmentation. The EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring.	
3.	General	Following functionalities are essential and required from such EMS tools: <ul style="list-style-type: none"> • Availability Monitoring, Management and Reporting • Performance Monitoring, Management and Reporting • Helpdesk Monitoring, Management and Reporting • Asset Management • Incident Management and RCA reporting Change and Configuration management	
4.	General	The Service Management solution to be used for incident and problem management, Inventory& Asset management, Service Request Management, Self Service, Service level management should be built to leverage the same common Configuration Management Database (CMDB) with a unified architecture	
5.	General	The service automation solution should provide configuration management and compliance assurance across servers, networks and applications	
6.	General	Solution should provide for future scalability of the whole system without major architectural changes	
7.	General	Solution should be distributed, and scalable and open to third party integration	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
8.	General	The solution should be able to monitor all the IT assets for the organization across all the location spread across including servers, network, routers, switches etc.	
9.	General	The agent and agentless monitor should be able to collect & manage event/ fault, performance and capacity data and should not require separate collectors	
10.	General	The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events	
11.	General	Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation	
12.	General	Should be configurable to suppress events for key systems/ devices that are down for routine maintenance or planned outage	
13.	General	The solution should provide the mechanism for creation of knowledgebase and provision the same to the end users with the ability to search for known errors from the knowledge base	
14.	General	The solution should provide network, server, application and database performance information and alarms and should be able to show it in a single console and provide a reporting interface for all network and system components	
15.	General	The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors	
16.	General	Database Monitoring: The solution should be able to monitor all the market leading database solution providers	
17.	General	The Database monitoring should seamlessly integrate with the same EMS dashboard/ Portal and provide integration with the central event console	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
18.	General	The tool should provide the organization the ability to easily collect and analyse specific information of applications & databases	
19.	General	The solution should manage service levels for delivery and support of business services	
20.	General	Should support compliance and cost trending to assist in identifying areas for process and operational improvements	
21.	General	Ability to create custom KPI metrics and scorecard/ compliance reports that are updated automatically	
22.	General	Single dashboard provides the as-is scenario by consolidating the data across the organization	
23.	General	Should support top down dashboards with drill down capabilities into detailed information	
24.	General	Should support comprehensive and configuration-level roll-back for changes	
25.	General	Should support cross-platform and reusable packaging with built-in rollback support	
26.	General	Should support Configuration-level Control of Tasks, Objects, and Policies	
27.	General	Should have ability to monitor the parameters and confirm compliance to security policies	
28.	General	Should have audit capabilities that compare the server status to policies defined in real-time/ scheduled basis	
29.	General	It should provide data filtration based upon user measurements (i.e., specific users, pages, requests, or transactions) to observe and analyse and track user activity at the individual or group level	
30.	General	It should automatically trends and provides dynamic performance baselines for applications and services	
31.	General	It should proactively identify errors affecting end-users, instead of waiting for a call from an employee or an incident being raised	
32.	General	It should provide comprehensive view of application performance from the end-user perspective; it should	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		distinguish between broad and targeted slow-downs, allowing drill-down into	
33.	General	The solution should look at a single user and track their activity across an application. Shows where problems are encountered, or why a particular instance of a page took a long time to load.	
34.	General	It should use real end user performance as one of the feed for more accurate root cause analysis and automated repair of business service performance issues	
35.	Technical	<p>Application monitoring parameters:</p> <ul style="list-style-type: none"> • Database Monitoring Attributes • User Connections (#) • Transaction Count • Log Space Available • Deadlocks/ sec • Database Free Space (%) • Database Used Space (MB) • Disk Reads (per sec) • Disk Writes (per sec) • Cache hit ratio • Lock Memory • Average Wait Time (per table) • Buffer Cache Hit Ratio (%) • Commits (per sec) • Memory Used (MB) • Percent Memory Used (%) • Availability (%) • Commits (per sec) • Percent Memory Used (%) • Buffer Cache Hit Ratio (%) • Active Instances (#) 	
36.	Technical	The proposed system shall support multiple types of discovery like IP range discovery including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
37.	Technical	<p>Web Server Monitors but not limited to:</p> <ul style="list-style-type: none"> • Post Requests (per sec) • Get Requests (per sec) • Errors (per sec) • Client-Side Errors (per sec) • Server-Side Errors (per sec) <p>Percent Busy Connections (%)</p>	
38.	Technical	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different parameters like CPU utilization, disk space, response times, resolution times (e.g. incident closed on 2 hours) performance and custom parameters of an enterprise etc.	
39.	Technical	The solution should have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance	
40.	Discovery, Configuration and Faults: Monitoring and Management	The proposed system shall support multiple types of discovery like IP range discovery including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices	
41.	Discovery, Configuration and Faults: Monitoring and Management	The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.	
42.	Discovery, Configuration and Faults: Monitoring and Management	The discovery shall be able to identify and model of the ICT asset.	
43.	Discovery, Configuration and Faults: Monitoring and Management	The proposed system shall provide a detailed asset report, organized by system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.	
44.	Monitoring and Management	The proposed system shall determine device availability and shall exclude outages from the	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		availability calculation with an option to indicate the reason.	
45.	Monitoring and Management	The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.	
46.	Monitoring and Management	The proposed solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise alarm when VM migrations happen between hosts.	
47.	Monitoring and Management	The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.	
48.	Monitoring and Management	The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.	
49.	Monitoring and Management	The proposed system shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.	
50.	Monitoring and Management	The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & start-up configuration, Upload configuration etc.	
51.	Reporting	The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.	
52.	Reporting	The proposed system shall able to perform real-time or scheduled capture of device configurations. It shall also provide features to capture, view & upload network device configuration.	
53.	Reporting	The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.	
54.	Reporting	The proposed system shall be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.	
55.	Reporting	The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.	
56.	Service Level Management: Monitoring and Management	The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the component and services provisioned as well as the SLAs.	
57.	Service Level Management	The system shall provide an outage summary that gives a high-level health indication for each service as well as the details and root cause of any outage.	
58.	Service Level Management	The system shall be capable of managing IT and Non-IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.	
59.	Service Level Management	The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).	
60.	Service Level Management	SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.	
61.	Service Level Management	The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		exempt any service outage from impacting an SLA shall be available.	
62.	Service Level Management: Reporting	The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.	
63.	Service Level Management: Reporting	The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.	
64.	Service Level Management: Reporting	The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box.	
65.	Service Level Management: Reporting	The System shall have all the capabilities of a Network Management System which shall provide Real-time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.	
66.	Network Performance Monitoring, Management and Reporting: Monitoring and Management	The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.	
67.	Network Performance Monitoring, Management and Reporting: Monitoring and Management	The tool shall have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices	
68.	Network Performance Monitoring, Management and Reporting: Reporting	This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
69.	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.	
70.	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. The following charts like mentioned below shall be available for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.	
71.	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.	
72.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes	
73.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall see response times based on different call parameters. For example, the proposed solution shall be able to provide CPU utilization metrics.	
74.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall give visibility into user experience without the need to install agents on user desktops.	
75.	Application Performance Monitoring,	The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
	Management and Reporting: Monitoring and Management		
76.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction	
77.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the Data center without having to rely on network monitoring tools.	
78.	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.	
79.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall address management challenges by providing centralized management across physical and virtual systems. The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.	
80.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.	
81.	Systems and Database Performance	It shall also be able to monitor various operating system parameters depending on the operating	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
	Monitoring, Management and Reporting: Monitoring and Management	system being monitored yet offer a similar interface for viewing the agents and setting thresholds.	
82.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.	
83.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started.	
84.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to act like sending an email.	
85.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.	
86.	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	It shall be able to automate monitoring, data collection and analysis of performance from single point.	
87.	Systems and Database Performance Monitoring,	It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
	Management and Reporting: Monitoring and Management	database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.	
88.	Systems and Database Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide Performance Management and Reporting Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines.	
89.	Systems and Database Performance Monitoring, Management and Reporting: Reporting	Role based Access Enables role-based management by defining access privileges according to the role of the user.	
90.	Systems and Database Performance Monitoring, Management and Reporting: Reporting	The proposed Virtual Performance Management system shall integrate latest virtualization technologies	
91.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.	
92.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	
93.	Helpdesk - Monitoring, Management and Reporting	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
94.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
95.	Helpdesk - Monitoring, Management and Reporting	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
96.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users. The proposed helpdesk system shall have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
97.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.	
98.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.	
99.	Helpdesk - Monitoring, Management and Reporting	It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
100	Helpdesk - Monitoring, Management and Reporting	Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket. It shall allow IT team to create solution & make them available on the end user login window for the most common requests	
101	Incident Management and Root Cause Analysis Reporting	An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process.	
102	Incident Management and Root Cause Analysis Reporting	Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.	
103	Incident Management and Root Cause Analysis Reporting	It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		details shall be accessible to relevant personnel as and when needed.	
104	Incident Management and Root Cause Analysis Reporting	Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.	
105	Incident Management and Root Cause Analysis Reporting	Conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).	
106	Incident Management and Root Cause Analysis Reporting	Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.	
107	Change and Configuration Management	Change and configuration management shall be governed by the change management and configuration management policy.	
108	Change and Configuration Management	Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.	
109	Change and Configuration Management	All changes shall be initiated using change management process; and a Request For Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.	
110	Change and Configuration Management	Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.	
111	Change and Configuration Management	The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.	
112	Change and Configuration Management	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.	
113	Change and Configuration Management	The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
114	Change and Configuration Management	The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.	
115	Change and Configuration Management	Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.	
116	Change and Configuration Management	Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.	
117	Change and Configuration Management	A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.	
118	Change and Configuration Management	Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hardware configuration images.	
119	Change and Configuration Management	Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hardware configuration images.	
120	ICT Assets Hardening	All the ICT assets shall be hardened as per the Hardening guidelines and industry leading practices. Remove all unauthorized software, utilities, and services. All required logs shall be configured and monitored.	

7.1.4 Identity Access Management Software (IAM)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	System shall be able to identify, authorize and authenticate the user and would allow access to the applications and database based on the user identity.	
2.	General	Identity and access management system would be able to identify the rights available with the user in terms of viewing, addition, deletion, modification of the data and generation of various reports through MIS.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	It would be possible to revoke the rights of users	
4.	General	The functionality for user maintenance such as creating users, creating teams, enabling and disabling users, deleting Users, assigning security roles to users, identifying managers for Users and assigning users to teams shall be considered	
5.	General	Single sign on and prioritizing key and normal users to be included as a part of IMS	
6.	General	Maintenance of the VPN users	

7.1.5 Directory Services

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Directory services would have a provision to create, update and modify the LDAP directory	
2.	General	It would have a provision to integrate with the Identity and access management	
3.	General	It would be used to define the roles and permission of different kinds of users in the system	
4.	General	Directory services would have proper integrations with DNS, DHCP, Email and other infrastructure components and services.	

7.1.6 Backup Solution

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The offered must support GUI with centralized management / Single interface for management of all backup activities.	
2.	General	Backup solution should be an image level backup software supporting popular hypervisors like VMware and Hyper-V Virtual Environments. Provide Block Level Incremental and Differential Backup and support Incremental and Differential Imaging.	
3.	General	Backup software should support application aware backups for all applications and databases hosted in the environment on physical/virtual servers with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup solution should be able to take backup on a unified storage from surveillance storage and all virtual machines/physical machines in the data centre.	
4.	General	Backup solution should store a backup recovery point as a single file.	
5.	General	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data.	
6.	General	The solution should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.	
7.	General	Solution should integrate with unified storage which is used for data backup with data deduplication capabilities.	
8.	General	The proposed backup solution should provide recovery from physical servers to Virtual and image level recovery.	
9.	General	Backup solution should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.	
10.	General	The offered solution license must be proposed as per solution for seamless access.	
11.	General	Premium support for the contract duration as per Industry Standard	
12.	General	Replication in the software should be a VM level replication and must replicate the VM level data with or without backing it up at the source site.	
13.	General	The proposed Backup software must allow to configure the maximum acceptable I/O latency level for production data stores to ensure backup and replication activities do not impact storage Availability to production workloads.	
14.	General	The software should be Network-efficient, Secure backup data replication with encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured without need of any other 3rd party WAN Accelerator requirements.	
15.	General	Licenses supplied should have support for Backup, Replication to DR site, and backup to minimum five MIETY approved Cloud Service Provider Platforms	

7.2 Antivirus

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Anti-virus shall have auto update feature, it shall be able to push signature from the centralized server to all the clients or workstations. The solution should have the ability to find whether the endpoint is out of compliance and should accomplish remediation, either via self-contained capabilities or integration with external resources	
2.	General	The solution must support mass mailing virus detection.	
3.	General	The solution must support mail attachment virus detection.	
4.	General	The solution must support Malformed Mail format detection.	
5.	General	Signature-based antivirus should eradicate malware on a system to protect against viruses, worms, Trojans, spyware, bots, adware, and rootkits.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
6.	General	The solution must have its own Updated Recommended Virus Extensions.	
7.	General	The solution must support Heuristics-based mail header detection for Spam.	
8.	General	Solution's on-premise sandbox must offer Malware detection by Static analysis, dynamic emulation, dynamic sandboxing using full (complete OS) virtual machines and thorough online reputational techniques	
9.	General	Solution should use a stateful attack analysis to detect the entire infection lifecycle. It should trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols, leading to data exfiltration.	
10.	General	The solution should utilize multiple detection approach by combining virtualization and emulation to capture more malicious behaviour across a wider range of custom environments.	
11.	General	Solution should have an emulator to cause threats to reveal themselves. This should not be a part of sandboxing and should run individually in each agent	
12.	General	The solution shall be able to act based on the category in which Spam is detected.	
13.	General	Proposed solution should support hybrid sandboxing (VM-based and emulated)	
14.	General	The proposed solution should support endpoint quarantine from network and bring back the endpoint after remediation using ATP management platform	
15.	General	The solution must support Encrypted Mail Detection.	
16.	General	The solution should manage single license for Windows, Linux and ac Operating Systems and management server should not be separate.	
17.	General	The solution must have a Secure SSL Web Management Console.	
18.	General	The solution must be able to prevent System Denial of Service Attack.	
19.	General	Solution should have application control, HIPS, Anti Malware being installed on single server. No separate servers and agents should be required for HIPS or application control	
20.	General	Solution should be able to turn on deception to add bait on the endpoints in your large, distributed environment without any additional agent by creating deceptors like remote connections, credentials, files, network shares, etc, so as soon as an attempt is made, you know you have an attacker	

7.3 Data Centre Infrastructure Management Software

7.3.1 Video wall management Software

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The software should be able to pre-configure various display layouts and access them at any time with a simple mouse click or based on the timer	
2.	General	The software should enable the users to see the desktop of the graphics display wall remotely on any PC connected with the Display Controller over the Ethernet and change the size and position of the various windows being shown.	
3.	General	The wall management software shall be having interoperability with Video management system.	
4.	General	The wall management software may be centrally Server based or local controller based architecture.	
5.	General	The software should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the Display Controller on the Ethernet	
6.	General	The software should copy the screen content of the PC / workstation connected on the Ethernet with the Display Controller to be shown on the Display wall in scalable and moveable windows in real-time environment.	
7.	General	Central configuration database	
8.	General	The Wall Control software shall perform health monitoring that allows timely detection of faults. <ul style="list-style-type: none"> • Wall health • Cube health • Cube IP-address • d. Brightness 	
9.	General	Wall Control Software shall allow commands on wall level or cube level or a selection of cubes: <ul style="list-style-type: none"> • Switching the entire display wall on or off • Fine-tune colour of each cube 	
10.	General	Log file functions	

7.3.2 Compute Virtualization and Management Solution (Compute)

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security.	
2.	General	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS) etc.	
3.	General	Live Virtual Machine migration between different generations of CPUs in the same cluster without the need for shared storage option and long distances from one site to another (up to 150 milliseconds round trip time) with no	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.	
4.	General	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another e.g.: FC, NFS, iSCSI, DAS	
5.	General	<ul style="list-style-type: none"> Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software. 	
6.		The solution design should ensure Zero or very minimal downtime based on SLA defined, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure through any means., without the cost and complexity of traditional hardware or software clustering solutions	
7.	General	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs	
8.	General	Create a cluster out of multiple storage data stores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time	
9.	General	<ul style="list-style-type: none"> VM-level encryption with no modifications in guest OS to protect unauthorized data access both at-rest and in-motion. The solution should also provide secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components. Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions 	
10.	General	<ul style="list-style-type: none"> Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions 	
11.	General	<ul style="list-style-type: none"> Span across a virtual datacentre and multiple hosts should be able to connect to it. This shall simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches. In-built enhanced host-level packet capture tool which shall provide functionalities like SPAN, RSPAN, and ERSPAN and shall capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
12.	General	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes	
13.	General	<ul style="list-style-type: none"> • Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data centre with single click • Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment. 	
14.	General	Direct OEM 24 X 365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.	
15.	General	<p>It should include proactive smart alerts with self-learning performance analytics Capabilities with Prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.</p> <ul style="list-style-type: none"> • Capacity analytics which can identify over-provisioned resources so that they can be right-sized and "What If" scenarios to eliminate the need for spreadsheets, scripts and rules of thumb, as well as Real-time, integrated dashboards of performance and capacity to enable a proactive management approach and help ensure SLAs are met • Automated workflow triggers which would let admins associate workflows created in Orchestrator layer with Operations alerts. For example, these workflows can automatically delete old VM snapshots when available capacity falls below a critical threshold or add resources when workload demands are rising above normal 	

7.3.3 Network and Security Virtualization

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Use hardware/software fabric manager /software Network Virtualization in complementary manner for providing secure and seamless underlay and overlay networking within the IT infrastructure as per their solution design.	
2.	General	Solution should be integrated with proposed virtualization solution so that it should allow for automated and on-demand creation of Network & Security policies which is scalable in nature.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	Solution should enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc.	
4.	General	The security policies should follow the Virtual Machines as they move within and between the virtual infrastructures so that there is no need of creation of security policies again for the applications once they move inside the datacentre.	
5.	General	Solution should protect every Virtual Machine with a state full distributed firewall.	
6.	General	The firewall-rule table of the solution should be designed for ease of use and automation with virtualized and container/microservices objects for simple and reliable policy creation	
7.	General	The solution should provide embedded distributed firewall and should provide near line rate performance	
8.	General	The solution should provide provisioning of virtual / software defined services and shall provide a VXLAN overlay solution independent of make and model physical network switches, routers and underlying network fabric with topologies like leaf and spine.	
9.	General	The solution should provide static and dynamic routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, L2 bridging to physical environments, L2 & L3 VPN services.	
10.	General	The solution should support extension of networking (Layer 2 extension) and security across data center boundaries irrespective of underlying physical topology enabling capabilities such as disaster recovery and active services recovery in to another DC or Public cloud.	
11.	General	The solution should be deployed in "N + 1 or N + 2" redundancy to provide availability as well as function so that even if one or two of the component fail, the remaining one shall function without any impact on data plane traffic.	

7.3.4 Building Management System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Solution for BMS: Solution should provide an appliance based pre-integrated, centralized and consolidated platform for end to end management of a building, which includes Facility infrastructure (HVACs, LT Panel- AMF, DG, UPS, Fuel Tank, CCTV, Fire Alarm and suppression system) along with IT infrastructure (network, server, application and database). The system should have the service dependency engine that allows to take intelligent decisions, as per the requirements. The tool should have the service oriented architecture layer and the mediation layer in a single plane. BMS should be open for third party integration via (soap, xml, web service, snmp-v1, v2, v3),	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		NO/NC ports (IO ports) and Modbus (TCP/IP&RTU) integration should be standard. For other industrial protocols, gateway integration should be available. The solution should perform the following general functions. But should be scalable with ready device certifications to accommodate new infrastructure getting added to the building	
2.	Visibility	It should get a single platform to manage the entire building and its components along with the integration with IT infrastructure. The way ahead should be drilling down to the component, which is under performing / about to fail or has failed. The impact of the failed equipment on others should get highlighted. We should get a Hawkeye view to know, how are all the building components working at any point of time. So that issues are addressed as quickly as possible.	
3.	Capacity	End equipment's in the building, should be set with thresholds to get an idea of how well they are rendering services to the people in the building. It should be able to proactively Identify potential area's which may need to be upgraded/downgraded (cooling, power, storage, etc.) with time. All vendor (end equipment vendors) SLA's and their respective maintenance contracts would be part of the OMS (operations and maintenance) plan.	
4.	General	Third Party Integration - for seamless data sharing to build a "Collaborative Decision Making System".	
5.	Salient Dependencies	Monitor & Control salient interdependencies between safety and security systems like: In case of fire, other than a fire alarm, we could get confirmatory information from the zonal camera. Multiple current surges in any particular zone should lead to an inspection of the electrical cables in the zone. Any sectional power failure, should help us to find the failure of the end equipment, by tracing down the LT panel SLD to the end equipment.	
6.	System with CMDB	Integrate people, process & technology. Decreasing the likelihood of downtime in the building by facilitating communication across all equipment's (part of the facility). A definite inventory management tool with a workflow system connecting responsible people, should be part of the solution.	
7.	Root-Cause Analysis	Isolate and pinpoint problem area before it impacts the building operations & business continuity while suppressing down the unwanted events.	
8.	General	Energy sources should always keep in check on the rated power consumption vs the power available for consumption. Since one of the big reasons for fire is higher load than the power distribution capability.	
9.	General	The solution should be capable to store the raw data or as-pollled data, for minimum of 365 days. It should also have	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
		the facility to automate the backup process or allow us to take manual backup, in case required.	
10.	General	The system should be capable of getting supported by the administrators at different levels. The system should provide individual and group rights and privileges. Normal users may have read access only, that too only to specific areas.	
11.	General	Support for email and SMS both (integration with SMS-gateway and GSM communication).	
12.	Energy Management	The system should be capable of integrating with the mains (LT panel), DG, UPS, PDU, rectifier, energy meters for continuous monitoring of its health. The battery health of the UPS would also be needed.	
13.	Energy Management	System should be able to do continuously monitor the quality of power, supplied to the electricity board and by the Generators (PF, frequency, harmonics distortion etc.), in order to avoid downtime.	
14.	Energy Management	System should have the feature to setup thresholds on each of the monitored energy parameter.	
15.	Energy Management	System should be able to clearly provide load trend for each rack, if need be in the building which would enable setup practical thresholds to get alerted on overload situations, in order to avoid any breakdown.	
16.	Fire Alarm System	The solution should proactively alert in case there is a possibility of an electrical fire (short circuit or over current)	
17.	Fire Alarm System	The solution should have the capability to integrate with different makes of fire alarm panels in the DCs and provide the alarms generated by the system on the centralized dashboard.	
18.	Fire Alarm System	The solution should be able to process a proper evacuation plan in-case of fire using the in-build rules engine.	
19.	Fire Alarm System	Trigger Audio and Visual alarm	
20.	Fire Alarm System	Co-relate with the nearest camera in the site with the FAS zone.	
21.	DG Monitoring & Fuel Automation	Proposed system should be able to integrate with diesel generators for measuring fuel level and run hours of the DG. System should also allow monitoring of various alarms (like: LLOP, dg on, etc.) including quality of power of the DG.	
22.	DG Monitoring & Fuel Automation	System should be capable to do fuel level monitoring of the diesel tanks installed for the gen-sets in the DC' building, in order to have a proactive estimation of fuel availability.	
23.	DG Monitoring & Fuel Automation	Mains Fail DG On DG Failed to start DG Failed to stop DG Fuel Level Low High Water Temperature	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		High Coolant Temperature Low Battery Voltage Low Lube Oil Pressure(LLOP)	
24.	Centralized Reporting & Dashboard	The dash board and reporting engine should provide centralized view for the entire infrastructure (physical security, safety & energy) and IT infrastructure (network, server, application and database) in the building.	
25.	Centralized Reporting & Dashboard	It should provide business users with highly interactive and power-users with highly sophisticated, pixel-perfect reports.	
26.	Centralized Reporting & Dashboard	It should provide Web-based interactive reporting for business users, Rich graphical report designer for power users, Parameterized reports with powerful charting, Output in popular formats: HTML, CSV, PDF, and ASCII.	
27.	Centralized Reporting & Dashboard	It should provide Analysis to explore data by multiple dimensions such as customer, product, network and time into the hands of business users.	
28.	Centralized Reporting & Dashboard	It should provide intuitive & rich graphic designer to create customized reports.	
29.	Centralized Reporting & Dashboard	Solution should provide a comprehensive centralized dashboard for health monitoring of Infrastructure components like: Electrical Panels, HVAC, UPS, and DG, Fuel etc. along with network, server, application and database.	

7.3.5 Access Control Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Central Management	The device shall allow registration of the fingerprints at a central computer using USB fingerprint scanner and software. Such fingerprint can be then distributed to any terminal in the network using synchronization process. Fingerprint data shall be stored in the central Database and Active Directory and shall support ASCL access control policies.	
2.	Fingerprint Technology	Proven and certified fingerprint recognition technology shall be used and each supplier needs to submit the details of original IPR holder for the Fingerprint Technology and International awards and recognition of the technology. For comparison sake we will only prefer technologies that have been tested in FVC competition as conducted by International bodies and accepted as most reputed competition in fingerprint industry	
3.	Software Backend	Software back-end shall have inter compatibility with LDAP V3 based Directory services for storing and managing the fingerprint data, which can be used for defining user policies based on Fingerprints for accessing servers / computers / premises	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
4.	Network Integration & Management	There shall be centralized management of all fingerprint time attendance systems. The system shall provide Centralized software for fingerprint registration, Storage of the entry and exit records in the centralized database as well as integration with Active Directory	
5.	Integrated TCP/IP	The device shall be based on advanced Networking architecture with Integrated Ethernet. It shall be possible to assign IP address/DHCP/Ports to the device from the Admin menu screen and automatically detect and configure the devices from central software without use of converters	
6.	Others	The centralized access control software shall support User Management, Door Control, Group Management, Real-time Door Monitoring, Terminal Management, Synchronization, Authentication Log Management, Batch User Downloading, System Log Management, Privilege Management, EXCEL report export, Time-zone Setting, User message Management, APB (Anti pass back) Setting, User Export/Import, Terminal Option Setting, Fingerprint Scanner Setting, Time Setting, Firmware Downloading and Basic T&A (Time & Attendance) Report	

7.4 Air Quality Management Software

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Environmental sensor station shall have a pre-installed software	
2.	General	Citizen can check the parameters through VaMS and Mobile App	
3.	General	System should give consolidated dashboard at City Operation Centre of ASCL	
4.	Application	System should be able to integrate with existing Environment sensors and (if applicable), and showcase a consolidated dashboard to ASCL	
5.	Application	The data should be collected in a software platform that allows third party software applications to read that data. 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.	
6.	Application	Software shall display real-time and historical data in chart and table views for dashboard view of the Client.	
7.	Application	Software shall display trends of environmental parameters based on user specific time periods.	
8.	Application	It shall be possible to configure and calibrate the sensors through the software from a remote location.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Application	Alarms shall be generated for events where the environmental parameters breach the safe or normal levels.	
10.	Integration	The integrated DDS software application shall allow user to publish specific messages & general informative messages.	
11.	VAMS	VaMS shall be integrated with the environmental station for automatically displaying information from environmental sensors.	
12.	VAMS	VaMS software application shall provide the normal operator to publish predefined sets of messages (textual / image) along with information from environmental sensors. The application shall have an option for supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.	

7.5 Surveillance Software

7.5.1 Video Management System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Video Management Server: Video Management System Servers shall maintain coherent operations between all servers and workstations. It shall host Management Server/s, Media / Recorder Server/s and Database Server/s.	
2.	General	Video Recorder Server: The Video Recorder Server shall be a dedicated server that shall store and process video with the help of Video Management System.	
3.	General	Video Analytics Server: Video Analytics Software shall be installed in the Video Analytics Server, to analyse live video in real-time to detect, identify, and track location, objects and people of interest. It shall automatically issue alerts to the appropriate personnel and initiate appropriate follow-up action according to predefined rules. This software shall also manage sensors; each sensor shall monitor a single video feed for security events. The video feeds shall be connected over the network to the Video Analytics Server. Sensors on the Video Analytics Server shall perform all event detection functions. Analytics shall also include ANPR and Face Recognition systems at the ICC.	
4.	General	Web Server(s) and Thick Clients: The system shall support Thick Client and Web Client to access the system.	
5.	General	The VMS architecture should comprise of centralised or decentralised architecture. The VMS should have system components such as Management Server to manage the system, Recorder or Media Server to stream and store the video feeds from the cameras and Database Server to store metadata information.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
6.	General	The VMS should support single site or multi-site deployment scenarios. The VMS should have capability to aggregate videos from multiple sites to the central site for recording or monitoring. The VMS should also have the capability to aggregate the system alerts such as video analytics, user created alerts and system health alerts to the central site.	
7.	General	The VMS should support single or multiple recorder server deployments. The proposed VMS should support unlimited IP and Analog cameras by augmenting the computing and storage hardware. The proposed VMS should support unlimited number of VMS clients.	
8.	General	The VMS architecture should support automatic assignment of the available cameras on the network to the available Recorder Servers based on the recorder server's resources such as number of cores, available RAM and resource utilisation.	
9.	General	VMS should be open to any IP and Analog cameras integration.	
10.	General	The VMS should be computing hardware agnostic and should work on commercially off the Shelf (COTS) servers and storage solutions.	
11.	General	The VMS should support virtual computing environment and should support all the industry leading virtualisation platforms available for Windows, Linux or Unix environment.	
12.	General	The VMS should support 64 bit architecture OS and hardware environments.	
13.	General	VMS shall store the system's configuration in a relational database, either on the management server computer or on the network.	
14.	General	The VMS should support redundancy at each level to avoid single point of failure. The redundancy should be built in to the platform and should offer failover support for Management Servers, Media / Recording Servers, Database Servers and Storage Medium.	
15.	General	VMS should support Failover against temporary disconnection of DBMS Service, without any loss of camera video. As soon as the DBMS service resumes, all data should automatically be synchronised to the Database.	
16.	General	Each media / recorder server should have its own storage configuration. It should be possible to select storage location/s out of all available storage locations (including Local, DAS, NAS, and SAN storage) for each media server. The media server should support load balancing and fail-safe operation by distributing the video data on all selected storage locations. So, in case of failure of any storage location, the entire video data is not lost.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
17.	General	The surveillance system shall provide a scalable and reliable platform to enable customized, network-based surveillance applications.	
18.	General	The VMS should support mix of storage technologies such as local / DAS / SAN / NAS storage. Each media server should support such storage locations simultaneously. RAID 6 shall be implemented on the Primary Video Recording Storage.	
19.	General	In case of the failure of the Recording Server, the VMS should automatically assign the cameras on the failed recording server to other operational/redundant recording servers on the network. Manual intervention of any kind should not be required in such a case. When the failed server becomes active again, the cameras should be automatically allocated to the recorder server again without manual intervention.	
20.	General	The Media Server should allow recording of camera feeds on network storage. In case the network storage fails, the recording server should start recording on the local storage. The local recording should get synchronised with the network storage as and when it is available again.	
21.	General	The system shall provide for integration with other software applications through an open and published Application Programming Interface (API). Such applications shall include, but not be limited to, access control, video analytics, incident management system and other alarm and sensor inputs. It shall be possible to integrate VMS into the Command & Control system.	
22.	General	VMS shall be open to any video wall system integration.	
23.	General	VMS should have Open Interface to send Analytics event alerts and other Maintenance Alerts (e.g. Camera disconnection, Storage Full, DBMS disconnection, etc.) over HTTP/HTTPS protocol to any external application running in a different machine in the same LAN. This is required for integration with command & control software or any other 3rd party incident management system.	
24.	General	This shall allow operations managers and system integrator to build customized video surveillance networks that meet the city requirements. VMS shall be a scalable and flexible video management system which should support unlimited cameras by adding licenses and augmenting the computing and storage infrastructure. The VMS should not have any cap on the number of client workstations.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
25.	General	VMS Server Management systems should support network time protocol (NTP) on server, which automatically sets the server time and date.	
26.	General	The Video Surveillance System should support high availability (HA) architecture.	
27.	General	VMS should support H.265+, H.265, H.264 and MJPEG stream for both live view and Recording independently. Compression rate should be manageable.	
28.	General	The VMS should have ONVIF Profile S & G compliance.	
29.	General	The VMS should be able to stream standard H.265+/H.265/H.264/Mpeg4 camera video streams to any external software on demand basis.	
30.	General	VMS video feeds shall be either directly encrypted or carried through encrypted tunnel using VPN or HTTPS (TLS 1.2) with FIPS 140-2 Approved Security Functions with end to end encryption technology from cameras to video recording servers.	
31.	General	The VMS should support ONVIF Profile G. The VMS should intelligently synchronise the edge recording on the camera with the central recording in case the camera loses the network connection.	
32.	General	Archive retention period should be configurable on per camera basis. The system should allow both retention based as well as First In First Out (FIFO) based deletion policy.	
33.	General	The VMS should support multiple directory access protocols such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP).	
34.	General	VMS should integrate with multiple mapping platforms such as Open Street Maps and Google Maps.	
35.	General	VMS should allow managing clusters of camera. Quantity of cameras per cluster should be unlimited. VMS should allow assigning each camera to one or several clusters simultaneously.	
36.	General	The Client Viewer should support real-time simultaneous view of 1, 2x2, 3x3, 4x4, 1+5, 1+7, 1+11, 8x8 multi-screens video display and a simple click should allow enlarging any of the multi-screen displays into a full screen display. On clicking again on the enlarged display, multi-screen display should reappear.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
37.	General	VMS should select the appropriate video stream from camera for display depending on the display resolution to optimize the network bandwidth.	
38.	General	The Client Viewer should support the use of standard PTZ controller or 3-axis USB joysticks for control of pan, tilt, zoom and auxiliary camera functions.	
39.	General	VMS should provide options for export format type (AVI/JPEG), timestamp, frame rate (full/half), digital zoom export, and AVI CODEC.Video clip may be exported to desktop/CD/DVD or a specific file path. All audio associated with the video being exported should automatically be included in the AVI export.	
40.	General	VMS should watermark every frame of the Video files with watermarks to authenticate the source of the video. While exporting video segments to external media (CD/DVD) or to any folder in workstations, the VMS should allow encryption of the video files.	
41.	General	The VMS desktop client should show vital system parameters for components such as Database Server, Media Servers, Local Workstation and Storage System (all available storages). The client should show the parameters such as CPU Core Usage, RAM Utilisation and Storage Utilisation.	
42.	General	The VMS should have reports such as camera uptime availability, camera recording percentage, recording status, critical events, incident video, etc.	
43.	General	The System health status like Server failure, Camera Disconnection, Storage Full Indication, etc. should always be displayed within the client workstation GUI all the time.	
44.	General	VMS should maintain a continuous log of Server Status Messages, Camera Connectivity, Storage Status, Recording ON/OFF, User Activity Logs, etc. which should be accessed from the workstations using different filters.	
45.	General	The system should give full audit trail of the user activities in the system.	
46.	General	The VMS should allow the user to bookmark any recorded video for ready reference at any later point of time.	
47.	General	The system should allow the user to tag critical Event clips so that they do not get removed from the storage based on FIFO/Retention period settings.	
48.	General	The VMS should allow multi-monitor support for the client workstation.	

7.5.2 Video Analytics

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.	
2.	General	The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.	
3.	General	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts	
4.	General	The system shall allow the configuration of applicable rules and manage them.	
5.	General	The system shall also enable editing the Zones and lines to the desired shape or size.	
6.	General	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event	
7.	General	The system shall enable masking of areas which interfere detection zones in other areas of the scene	
8.	General	The system shall enable detecting rules in the defined areas (zones/ lines)	
9.	General	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.	
10.	General	The system shall be able to filter large amounts of video and focus on human attention appropriately	
11.	General	The system shall allow classification of different objects like animals, vehicles, people etc.	
12.	General	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.	
13.	General	VA shall provide secured feeds with encryption, watermarking for data authenticity	
14.	General	VA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.	
15.	General	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system	
16.	General	VAS should allow to add, edit, delete or disable and enable Policies.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
17.	General	<p>The city-wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day 1.</p> <p>Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA), Unattended object, Object Classification, Tripwire / Intrusion, Loitering, etc.</p> <p>Vehicle Wrong Way Detection, Illegal Parking Detection, Congestion Detection, Vehicle Counting, Speeding Detection, Parking Management etc.</p> <p>Video Stitching with Object Tracking, Video Stabilization, Video Smoke Detection, Video Fire Detection etc.</p> <p>Crowd Control, Counter-Flow Detection, People Counting, Line Control, People Tracking etc.</p>	
18.	General	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)	
19.	General	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification	
20.	General	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.	

7.5.3 Face Recognition System

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system.	
2.	General	The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real-time report such as Audit log report, Hit List Report, Daily Statistics Report and Distribution Report etc.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	The facial recognition system should be accessible from 5 different desktops / laptops at any given time. When choosing a distributed architecture, the system shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision.	
4.	General	The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts.	
5.	General	The algorithm for facial recognition or the forensic tool should be able to recognise partial faces with varying angles	
6.	General	The system should be able to detect multiple faces from live single video feed	
7.	General	The system should have combination of eye-zone extraction and facial recognition	
8.	General	The system should have short processing time and high recognition rate	
9.	General	The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)	
10.	General	Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall use of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.	
11.		The system should be able to identify and authenticate based on individual facial features	
12.	General	The system should have capability for 1:1 verification and 1:N identification matching	
13.	General	The system should be able to support diverse industry standard graphic and video formats as well as live cameras	
14.	General	The system should be able to match faces from recorded media.	
15.	General	The system should be able to detect a face from a group photo	
16.	General	The system should be able to detect a face from stored videos of any format	
17.	General	The system should have bulk process of adding faces in the system	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
18.	General	The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing.	
19.	General	The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for windows OS or android OS to capture a face on the field and get the matching result from the backend server.	
20.	General	The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas.	
21.	General	The system shall be able to detect faces in different environmental changes like rain, wind, fog and poor light.	
22.	General	The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".	
23.	General	FRS should cover the following features: i. Face Capture ii. Face Counting iii. Face Recognition	
24.	General	Facial Image Database Management: It should allow users to manage the facial image library, including registering, changing, deleting & querying facial image information	

7.5.4 ANPR Server Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Vehicle Detection and Video Capture Module	<ul style="list-style-type: none"> The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition. The System should automatically detect the license plate in the captured video feed in real-time. The system should perform Optical Character Recognition (OCR) of the license plate characters. The System should store JPEG image of vehicle and license plate and enter the license plate number into database management system like MSSQL, MySQL, and PostgreSQL etc. along with date timestamp and site location details. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> System should be able to detect and recognize the English alpha numeric license plate in standard fonts and formats for classes of vehicles such as cars, HCV, and LCV. The system should be robust to variation in License Plates in terms of font, size, contrast and colour and should work with good accuracy 	
2.	Vehicle Detection by Colour	<ul style="list-style-type: none"> The system should detect the colour of all vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colours. The system should store the colour information of each vehicle along with the license plate information for each transaction in the database. The system should have options to search historical records for post event analysis by the vehicle colour or the vehicle colour with license plate and date time combinations. 	
3.	Alert Generation	<ul style="list-style-type: none"> The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel. The system should be able 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 	
4.	Vehicle Status Alarm Module	<ul style="list-style-type: none"> On successful recognition of the number plate, system should be able generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need). The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user. 	
5.	Vehicle Log Module	<ul style="list-style-type: none"> The system should enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports should include: 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> • 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. • The system should have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities. • The system should have option to save custom reports for subsequent use. The system should have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems. • The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1 and 2-character distance). 	
6.	Vehicle Category Editor	<ul style="list-style-type: none"> • The system should have option to input certain license plates according to category like "Wanted", "Suspicious", "Stolen", and "Expired" etc. by Authorized personnel. • The system should have an option to add new category by authorized personnel. • The system should have option to update vehicle status in specific category by authorized personnel. E.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved". • System should have option to specify maximum time to retain vehicle records in specific categories. 	
7.	Central Management Module	<ul style="list-style-type: none"> • The Central Management Module should run on the ANPRS Central Server in control booth. It should be possible to view records and edit hotlists from the Central Server 	
8.	Centralized Video Management Module	<ul style="list-style-type: none"> • Besides recording the snaps & video clips of every license plate extracted, it is also required that a centralized video management software is also supplied to achieve the below: - • Continuous recording of every lane video irrespective of presence of vehicle. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> Such recording schedules can be continuous, event based, schedule based, trigger based etc. Archive Search using dates, time, event etc. High Availability/Redundancy of Recording & Database. Health monitoring module - To allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices. The health monitoring module should provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting. Virtual Matrix – To allow viewing of live video in different layouts on operator screen. Video stitching – It should allow stitching of multiple lane videos/tiles to provide panoramic type seamless view of both entry & exit lanes. The centralized Video Management Module should be part of same ANPR software framework. No 3rd party VMS is allowed to be offered, howsoever integrated it may be 	

7.5.5 Public Announcement Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	<ul style="list-style-type: none"> Software shall be fully proven prior to being supplied, installed, tested and commissioned. A list of reference sites at which the system software has been installed and operational at the date of the closing of this tender shall be provided. The operator interface software shall incorporate English language descriptions and messages using both text based menus and graphical/icon displays. All configuration (e.g. entering of alarm response properties, adjusting time schedules, user data, etc.) shall be performed on-line without effecting the operation of the overall system. Selective access to different operator functions shall be configured based on an operator's user level. User levels shall be determined from the Biometric verification each time an operator logs on to a workstation. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> • After any predefined period, if no operator activity has occurred at the operator workstations, that station shall automatically request Biometric verification failing which the station shall log off. • The time period before automatic logging off of workstations shall be user configurable, and shall be determined during commissioning of the system, in liaison with the Engineer. 	
2.	Operating System	<ul style="list-style-type: none"> • The operating system shall be a recognised and widely accepted standard operating system that shall suit the requirements of the system to be installed. The operating system shall be a real-time multi-user/multi-tasking system such as NT, W2000, UNIX or QNX. The operating system shall have proven and demonstrated reliable operation in the security environment. • Facilities shall be provided to store all programs on site and include all equipment necessary to backup and reload all system programs, including the operating system with all user specific system parameters. 	
3.	System Access	<ul style="list-style-type: none"> • Operators shall be required to "log on" to operator workstations using the finger print reader provided at each operator station before being able to access the system or user information, reset alarms or access any other system functions. • Access to all workstations shall be limited through allocation of access levels. • A minimum of 100 users and 100 User levels shall be available. Only users allocated with a user level of 99 shall be capable of the assignment and changing of passwords to all levels. • Each operator shall be allowed to access different operator commands and functions, and view certain individually assigned events, menus and functions based on their assigned user level. 	
4.	System Reporting	<ul style="list-style-type: none"> • The GUI shall be capable of performing SQL queries to the current or archived databases on the server workstations, format the data into customised reports which shall allow for the following: • Display of all relevant information on any individual alarm point including alarm point identification by device number and alarm point status. 	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		<ul style="list-style-type: none"> • Display all alarm points in the system in alarm or normal condition, as a single log. • Display all emergency procedures applicable to any alarm type with corresponding alarm response actions and locations, per alarm device. • Reporting details shall include: <ul style="list-style-type: none"> • Alarm point status • Alarm count per device. • Alarm activity over a time period, selected by time and date. • Display of selected alarm transactions based on alarm type and a calendar / time period. • Display system operators login/out history • Display all operator commands entered by any or all operators based on time/calendar interval. 	
5.	System Status	<ul style="list-style-type: none"> • The GUI shall provide a menu option which, when selected, allows the system to display or print a list of current alarms, faults and conditions including the current fault conditions relating to GUI workstations and Intercom system hardware. • In graphical display mode the system shall display maps of each building complete with all internal levels and shall indicate all systems equipment status (i.e. Intercom on, off, tamper, Threshold, isolated etc.) 	

7.5.6 Body Camera Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	Body camera software shall be provided at the ICCC and as a single standalone installation on a local PC or laptop that can be installed on any police location.	
2.	Encryption	Software shall provide AES encryption, ensuring files are completely secure, and a full audit trail to protect the evidential integrity of the videos you capture. Access to the software shall be password protected, and multiple user access levels can be allocated dependent on requirements.	
3.	Functionality	Searching and organising files shall be completely intuitive. Files shall be sorted and searchable by vital metadata such as date, time, location, device number and	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
		user. It shall also allow adding custom tags to files to make them even easier to find	
4.	Password protected	The software shall provide password protected access	
5.	Role based	Set designated administration levels and user access rights	
6.	Manage your files	Organise and search for your files using detailed metadata	
7.	Share	Collaborate on cases by securely sharing case files	
8.	Data Protection	Files are deleted after 30 days (configurable) unless required for ongoing case	
9.	Evidential usage	Provides full audit trail so your files are evidentially sound	

7.6 Waste Water Quality Management Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	OWQMS shall consist of a web based application and mobile application to provide systematic framework for enhancing waste water discharge monitoring to detect emerging water quality issues and respond prior to the problem occurs in the city.	
2.	General	OWQMS shall utilize real-time water quality parameters collected from quality sensors across the drainage canals to analyse and detect waste water quality anomalies.	
3.	General	Monitoring shall include all the waste water quality parameters received from the remote sensors.	
4.	Data Communication	Waste water quality parameters shall be fetched from the Intelligent Gateway via 3G/LTE network.	
5.	Data Communication	The system shall have the desired interfaces for the data integration with other existing applications as necessary. It shall be possible to integrate with State and Central Pollution Boards portals/database via API integration to share waste water quality data.	
6.	Data Communication	The application shall import and store sensor measurement and state data (operational and communication status) at a specified time frequency from other relevant databases and systems to analyse, and visualize the waste water quality data on a continuous basis.	
7.	Information Management & Analysis	Based on operational and communication status and other characteristics, it shall determine whether data is valid or invalid, and whether the quality of the data is sufficient to assess waste water quality.	
8.	Information Management & Analysis	Shall analyse valid sensor data to assess water quality and sensor states.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
9.	Information Management & Analysis	Shall perform advanced data analysis, such as time-series trend analysis, multi-parameter clustering, and single parameter thresholding for identifying unusual waste water quality events due to either intentional or unintentional causes	
10.	Alert Investigation	Shall generate and manage alarms based on sensor states and waste water quality determined by the analysis of a) valid sensor data and b) calculated water quality parameters	
11.	Alert Investigation	Shall generate email and SMS notifications, follow-up notifications, and escalated notifications to appropriate personnel in the event of alarms	
12.	Reports	Shall generate standard and user-configured reports.	
13.	Reports	Shall have the control access to all data, results, reports, and system administration tools	

7.7 Helpdesk Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.	
2.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	
3.	Helpdesk - Monitoring, Management and Reporting	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
4.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
5.	Helpdesk - Monitoring, Management and Reporting	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	
6.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
7.	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.	
8.	Helpdesk - Monitoring, Management and Reporting	It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
9.	Helpdesk - Monitoring, Management and Reporting	Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket. It shall allow IT team to create solution & make them available on the end user login window for the most common requests	
10.	Incident Management and Root Cause Analysis Reporting	An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process.	
11.	Incident Management and Root Cause Analysis Reporting	Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.	
12.	Incident Management and Root Cause Analysis Reporting	It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.	
13.	Incident Management and Root Cause Analysis Reporting	Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.	
14.	Incident Management and Root Cause Analysis Reporting	Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.	

7.8 Variable Message Display Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	The Software powers up the Media Player at pre-determined times on all functioning days of the Station	
2.	General	The Software powers off the unit during the closing hours of the Station	

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	No Personnel should be required to either switch on, switch off, power off, log in or log out procedures. All the above functions should function automatically as scheduled	
4.	General	Multiple Screen Layouts with Multiple Independent Zones.	
5.	General	Play Standard Multimedia Files: Flash, Videos, Images, etc.	
6.	General	Separate Weather Banners	
7.	General	Scrolling Banners	
8.	General	Time-Sensitive Content – Expired old content to be purged	
9.	General	Unattended, Continuous Playback	
10.	General	Remote Shutdown, Reboot Mode	
11.	General	Connect on “as-and-when-needed” basis	
12.	General	No Proprietary Hardware required	
13.	General	Off the Shelf Operating Systems	
14.	General	Scalable Network	
15.	General	No need of dedicated bandwidth	
16.	General	Play Scheduled Playlist in day parts	
17.	General	Ability to schedule permitted download and upload time so as to use connectivity during non-peak hours	
18.	General	Proof of Play and Log Retrieval	
19.	General	Support Major Indian Language Fonts	
20.	General	24 X 365 Operations	

7.9 Sewerage Treatment Plant Integration

7.9.1 SCADA HMI Software

S. No.	Parameter/requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	SCADA HMI software shall be the extended client software of existing SCADA server (GE-CIMPLICITY V9.0) at Sewerage Treatment Plant (STP) using web based interface.	
2.	General	SCADA HMI Client at ICCC shall be able to connect to the SCADA HMI server over a secured VPN network.	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
3.	General	The software shall have the object library with advance feature for richer user experiences.	
4.	General	It shall support .NET/WPF in viewer. The software shall have the web interface support for accessing through browsers.	
5.	General	Existing HMI screens at STP shall be accessible and monitored at ICCC using this SCADA HMI client software.	
6.	General	It shall have the feature to access / engineer the graphics for dynamic display. The Digital Graphical Replay add-on feature shall provide the ability to replay Historical events.	
7.	General	It shall allow to create templated applications for repeatable assets, which can be leveraged in both existing clients and new Web HMI.	

7.9.2 VPN Software (for Client-Server Connection)

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	General	VPN Server client software shall be supplied and deployed for the connection establishment of SCADA HMI client at ICCC from each individual STP.	
2.	General	It shall provide secure communication over broadband, wireless and dial-up connections.	
3.	General	It shall have the VPN client feature easy-to-follow wizards to help users to help user quickly and easily install the product and configure VPN client connection streamlining the VPN deployment and Management.	
4.	General	It shall support ESP (Encapsulated Security Payload) over IPsec modes	
5.	General	It shall support DES / 3 DES Encryption Algorithm	
6.	General	Data Integration shall be based on MD5, SHA1	
7.	General	It shall have the network security feature to secure network access flexibility by allowing IPsec VPN to pass through any IP Network using NAT	
8.	General	It shall have simple user interface, the Global VPN Client offers point-and click VPN activation and streamlined management tools to minimize support requirements	
9.	General	VPN client shall allow Secure, Reliable, client-initiated VPN connections	
10.	General	It shall support user authentication service for login authentication	

7.10 Business Continuity Management Software

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
1.	Access	Web based access with compatibility with Active Directory for Employee's information details and SMS, Auto phone dialler systems for emergency notification. (Shall not store data in cloud data storage/DB).	
2.	Access	Different levels of privileges to access BC Documents & records	
3.	Access	Different levels of authorization / approvals in the system for BC activities and documents.	
4.	Access	Access Control – issue and maintenance of user ids & passwords Mobile application compatibility with Android and IOS.	
5.	Function	Full BCMS framework as per ISO 22301 with the ability to customize documents & methodologies.	
6.	Function	Auto-uploading of BC documents data.	
7.	Function	Carry out BIAs including process level risk assessment & single point of failures	
8.	Function	Conduct BC Risk assessment for sites / locations with an option to select multipliable BC strategies.	
9.	Function	Manage and coordinate incident response / crisis management plan and carry out post-incident reviews.	
10.	Function	Carry out tests / exercises including call tree (test plans, schedules & test results)	
11.	Function	Carry out bench marking activities, record of continual improvements.	
12.	Function	Ability to add / change / modify business processes without deletion / creation of new documents within the same year.	
13.	Function	Ability to carry out audit, maintain audit trails and tracking of audit observations till closure	
14.	Reporting and Printing	Auto-generation of mails for activities based on frequency / periodicity.	
15.	Reporting and Printing	Labelling of reports based on confidentiality.	
16.	Reporting and Printing	Consolidated Report of open issues emerged during testing / exercising and actual incidents	
17.	Reporting and Printing	Printing of BC Documents in pdf, word and excel sheets	
18.	Reporting and Printing	Ability to print full versions or selected pages of BC Plans	
19.	Reporting and Printing	Create Top Management Reporting (MIS) which include:	
20.	Reporting and Printing	Consolidated Business Impact Analysis and Risk Assessment reports sorted by business criticality highlighting business requirements and provides sub reports which can be extracted as following:	

S. No.	Parameter/ requirement	Minimum specifications/requirements	Compliance (Yes / No)
21.	Reporting and Printing	Business RTO / RPO Vs Technology Application / System RTO & RPO.	
22.	Reporting and Printing	Strategy wise location / business wise report	
23.	Reporting and Printing	BCP Seat availability location / business wise.	
24.	Reporting and Printing	Test schedule and completion result.	
25.	Reporting and Printing	Call Tree Test schedule and completion result.	
26.	Reporting and Printing	MIS report (based on KPIs) with a summary of the status in pie chart / graph.	
27.	Reporting and Printing	Different type of reports can be extracted for saving and printing purpose (pdf, word and excel sheets).	

8 Appendix V: Indicative locations for Field equipment

Indicative location for IP Camera, Public Address System, Emergency Call Box and Variable Message Display Boards

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
1.	Commissioner of Police, Amritsar	Administrative Building	-	-	-	-	2	-	-	-
2.	District HQ, Amritsar	Administrative Building	-	-	-	-	2	-	-	Yes
3.	PUDA Bhawan	Administrative Building	-	-	-	-	2	-	-	-
4.	General & Textile Union	Administrative Building	-	-	-	-	2	-	-	-
5.	T point airport road	Airport Entry / Exit Point	4	-	-	-	3	-	-	-
6.	Bus stand (In gate towards bus stand waiting area)	Bus Stand	-	-	-	-	-	1	Yes	Yes
7.	Bus stand (Out gate towards outside from waiting area)	Bus Stand	-	-	-	-	-	1	Yes	-
8.	Bus stand (Centre inside the parking area)	Bus Stand	-	-	-	-	-	1	Yes	-
9.	Outer Gate Bus stand	Bus stand	2	2	-	-	-	1	-	-
10.	Amritsar Bus stand (ISBT)	Bus stand	2	6	-	-	-	3	-	-
11.	Verka Bus Stop	Bus stop	2	2	-	-	4	-	-	-
12.	Adda fatehpura	City Entry/ Exit Point	4	-	-	-	4	1	-	Yes
13.	T-Point Fatehsingh Colony Fatehpura Road	City Entry/ Exit Point	4	-	-	-	4	1	-	-
14.	Amritsar Entrance	City Entry/ Exit Point	4	-	-	-	4	1	-	Yes
15.	Tarawala Bridge	City Entry/ Exit Point	-	-	-	-	4	1	-	-
16.	Gururamdas Hospital Vallah Gate	City Entry/ Exit Point	4	-	-	-	4	1	-	-
17.	Chowk Mudal Bypass	City Entry/ Exit Point	4	-	4	-	-	1	-	-
18.	India Gate Chehta Road	City Entry/ Exit Point	4	-	-	-	3	1	-	-
19.	Sunsahab Gurudhwara	City Entry/ Exit Point	2	-	-	-	4	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
20.	Mahal PP	City Entry/ Exit Point	4	-	-	-	3	1	-	-
21.	Sharah Baba Deepsingh ji Shidhawala	City Entry/ Exit Point	4	-	-	-	3	1	-	-
22.	Majitha Chowk Bypass	City Entry/ Exit Point	4	-	-	-	4	1	-	-
23.	Amritsar Toll Plaza, Manawala	City Entry/ Exit Point	2	-	-	-	4	1	-	-
24.	Chhattiwind Nehar	City Entry/ Exit Point	2	-	-	-	4	1	-	-
25.	Saroop rani govt college	College	-	-	-	-	2	-	-	-
26.	Khalsa College Women	College	-	-	-	-	2	-	-	-
27.	Khalsa College	College	-	-	-	-	2	-	-	-
28.	GND University	College	-	-	-	-	3	-	-	-
29.	Ranjit Avenue ITI College	College	-	-	-	-	3	-	-	-
30.	Guru Ram Das Dental College 100 Ft Road	College	-	-	-	-	2	-	-	Yes
31.	Bedi School	College	-	-	-	-	3	-	-	-
32.	Shehzada Nand College Green	College	-	-	-	-	2	-	-	-
33.	IKGPTU Campus Amritsar	College	-	-	-	-	2	-	-	-
34.	Central Institute of Plastics Engineering and Technology	College	-	-	-	-	2	-	-	-
35.	Indian Institute of Management	College	-	-	-	-	2	-	-	-
36.	Katrabhai Sant Singh Chowk	Crime Hotspot	1	-	2	-	-	-	-	-
37.	Majith Mandi Chowk	Crime Hotspot	-	-	-	-	-	1	-	Yes
38.	Chowk Chaursti Attari	Crime Hotspot	1	3	-	-	-	-	-	-
39.	Balmik Mohalla	Crime Hotspot	1	-	3	-	-	-	-	-
40.	Main Road bangla basti	Crime Hotspot	1	2	-	-	-	-	-	-
41.	Chabal Road Railway Crossing	Crime Hotspot	1	-	2	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
42.	City Centre Back Side	Crime Hotspot	1	-	2	-	-	-	-	-
43.	Ram Bagh	Crime Hotspot	1	-	2	-	-	-	-	-
44.	Ram Talai	Crime Hotspot	1	-	2	-	-	-	-	-
45.	Sultanwind chowk (Amritsar Entrance Village)	Crime Hotspot	1	-	2	-	-	-	-	-
46.	Bhagtwala Chowk	Crime Hotspot	1	-	2	-	-	-	-	Yes
47.	Jora Fatak	Crime Hotspot	1	-	5	-	-	-	-	-
48.	Dholimala T-Point	Crime Hotspot	1	-	3	-	3	-	-	-
49.	Putlighar Chowk	Crime Hotspot	1	2	-	-	-	1	-	-
50.	Rani ka Bagh Near Gift Shop	Crime Hotspot	1	-	2	-	-	-	-	-
51.	Kamal Mahajan Hathi Gate	Crime Hotspot	1	-	2	-	-	-	-	-
52.	100 Feet Sowadi Road	Crime Hotspot	-	-	-	-	4	1	-	-
53.	Sunena Bazar, Guru Bazar	Crime Hotspot	-	-	-	-	2	1	-	-
54.	Sheeda Sahib Gurudwara	Crime Hotspot	-	-	-	-	2	1	-	-
55.	Jahazgarh, ANPR	Crime Hotspot	-	-	-	-	2	1	-	-
56.	Transport nagar	Crime Hotspot	-	-	-	-	2	1	-	-
57.	Focal Point 1-2	Government Infrastructure	-	-	-	-	8	-	-	-
58.	Chowk Milk Plant Verka	Government Infrastructure	-	-	-	1	-	-	-	-
59.	Suvidha Centre (North	Government Infrastructure	-	-	-	1	-	-	-	-
60.	Sewerage Treatment Plant (Location 1, to be decided)	Government Infrastructure	-	-	-	1	-	-	-	-
61.	Sewerage Treatment Plant (Location 2, to be decided)	Government Infrastructure	-	-	-	1	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
62.	Sewerage Treatment Plant (Location 3, to be decided)	Government Infrastructure	-	-	-	1	-	-	-	-
63.	Govt Medical College Majitha Road Medical Avenue	Hospital	-	-	-	-	2	-	-	-
64.	Chikitsa ENT Hospital Pink Plaza	Hospital	-	-	-	-	2	-	-	-
65.	Civil Hospital	Hospital	-	-	-	-	4	1	-	-
66.	District Shopping Complex Parking	Main Markets Entry	-	-	-	-	6	-	-	-
67.	Pink Plaza	Main Markets Entry	-	-	-	-	2	-	-	-
68.	Machhi Mandi Market	Main Markets Entry	-	-	-	-	2	1	-	-
69.	Shimla Market	Main Markets Entry	-	-	-	-	2	1	-	-
70.	Alpha One Mall	Main Markets Entry	-	-	-	-	3	2	Yes	-
71.	Trillium Mall	Main Markets Entry	-	-	-	1	-	2	Yes	-
72.	Celebration Mall	Main Markets Entry	-	-	-	-	3	2	Yes	-
73.	Sultan Wind Clothes Market	Main Markets Entry	-	-	-	-	3	1	-	-
74.	Bhadar Kalimandir Khajan Gate	Main Markets Entry	-	-	-	-	3	1	-	-
75.	Model Twon Mandir	Main Markets Entry	-	-	-	-	3	1	-	-
76.	Company Bagh	Main Markets Entry	-	-	-	-	2	3	-	-
77.	Gurunanak Stadium	Main Markets Entry	-	-	-	-	2	1	-	-
78.	Beri Gate Market Pal Vala Area	Main Markets Entry	-	-	-	-	2	1	-	-
79.	Putligarh Market Area	Main Markets Entry	-	-	-	-	2	1	-	-
80.	Vallah Mandi Area	Main Markets Entry	-	-	-	-	5	3	-	-
81.	Hall Bazaar (Location 1, to be decided)	Market	-	-	-	-	-	1	Yes	-
82.	Hall Bazaar (Location 2, to be decided)	Market	-	-	-	-	-	1	Yes	-
83.	Hall Bazaar (Location 3, to be decided)	Market	-	-	-	-	-	1	Yes	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
84.	Queens road (Location 1, to be decided)	Market	-	-	-	-	-	1	Yes	-
85.	Queens road (Location 2, to be decided)	Market	-	-	-	-	-	1	Yes	-
86.	Giani Tea Stall vicinity	Market	-	-	-	-	-	1	Yes	-
87.	Putligarh – kichloo chowk – Khandwala chowk (20 mtrs - 30 mtrs)	Market	-	-	-	-	-	1	Yes	-
88.	Lohgarh chowk	Market	-	-	-	-	-	1	Yes	-
89.	Link road	Market	-	-	-	-	-	1	Yes	-
90.	Drama Wala bazar	Market	-	-	-	-	2	-	-	-
91.	Chora bazar	Market	-	-	-	-	1	-	-	-
92.	Chungiwala bazar	Market	-	-	-	-	1	-	-	-
93.	Choti dhab bazar (Shivsanti)	Market	-	-	-	-	2	-	-	-
94.	Sutto wala bazar	Market	-	-	-	-	3	-	-	-
95.	Guru Bazar chowk	Market	-	-	-	-	2	-	-	-
96.	Purani Sabji Mandi	Market	-	-	-	-	2	-	-	-
97.	Sabji Mandi samasan Ghat	Market	-	-	-	-	3	-	-	-
98.	Hotel Best western	Market	-	-	-	-	2	1	-	-
99.	T-Point MK Hotel	Market	-	-	-	-	2	-	-	-
100.	Ranjit Avenue Chowki	Market	-	-	-	-	2	-	-	-
101.	C-Block Chowk Ranjit Avenue	Market	-	-	-	-	2	-	-	-
102.	Shimla Market	Market	-	-	-	-	2	-	-	-
103.	Amritnal Bagh (Rose Garden)	Park	-	-	-	-	2	-	-	-
104.	S.Raminder Singh Bulariya Park	Park	-	-	-	-	3	1	-	-
105.	Park Guru Govind singh Nagar	Park	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
106.	Arya Samaj School Park	Park	-	-	-	-	2	1	-	-
107.	Open Space Sewa Kendra Opp Arya Samaj School Park	Park	-	-	-	-	2	1	-	-
108.	Peripheral Park	Park	-	-	-	-	6	1	-	-
109.	Gang Di Mori Park	Park	1	-	2	-	-	1	-	-
110.	Sant Nagar Park Dolphin Park	Park	-	-	-	-	2	1	-	-
111.	Gali Munshiyaan Rodanwali	Park	-	-	-	-	2	1	-	-
112.	Gali Hargobindpura	Park	-	-	-	-	2	1	-	-
113.	Shastri Nagar, Park Lawrence Road	Park	-	-	-	1	-	-	-	-
114.	Park Canady Avenue	Park	-	-	-	1	-	-	-	-
115.	Dump Dump School, Tehsilpura	Park	-	-	-	1	-	-	-	-
116.	Kashmir Avenue, Rose Garden	Park	-	-	-	1	-	-	-	Yes
117.	Dhingra Complex, Near Panj Peer, G.T. Road	Park	-	-	-	1	-	-	-	-
118.	Park Chamrang Road, B/S Mata Kauhal Hospital	Park	-	-	-	1	-	-	-	-
119.	Sakatri Bagh	Park	-	-	-	1	-	-	-	-
120.	Hindu Shaba Sen. Sec. School, Amritsar	Park	-	-	-	1	-	-	-	-
121.	Shubash Park, Katra Sher Singh	Park	-	-	-	1	-	-	-	-
122.	Gurbkash Nagar, Green Park, Near Police Chowki,	Park	-	-	-	1	-	-	-	-
123.	Mahadev Vidiya Niketan School, A-Block, Ranjit Avenue	Park	-	-	-	1	-	-	-	-
124.	Bent Park, Opp MK Hotel	Park	-	-	-	1	-	-	-	-
125.	Golbagh	Park	-	-	-	1	-	-	-	-
126.	Moon Avenue, Sharma Park	Park	-	-	-	1	-	-	-	-
127.	Akash Avenue, Near DhamMandir Near Bypass	Park	-	-	-	1	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
128.	Trikoni Park, Rani ka Bagh	Park	-	-	-	1	-	-	-	-
129.	Guruduara Singh Sahib, Rani Ka Bagh, opp. Park	Park	-	-	-	1	-	-	-	-
130.	Government High School, Gate Hakima	Park	-	-	-	1	-	-	-	-
131.	B-Block, Railway Colony Park	Park	-	-	-	1	-	-	-	-
132.	Green Avenue market	Park	-	-	-	1	-	-	-	-
133.	Park Basant Avenue	Park	-	-	-	1	-	-	-	-
134.	Tripti Bala ji Mandir, Green field, Majitha Road	Park	-	-	-	1	-	-	-	-
135.	Gopal Nagar Near Hari Mandir, Tanki wali Gali, Majitha Road	Park	-	-	-	1	-	-	-	-
136.	Joshi colony	Park	-	-	-	1	-	-	-	-
137.	Park Wali tanki, Near Japani Mills, Main Road Chheharta	Park	-	-	-	1	-	-	-	-
138.	Shiva Ji Park, Rani ka Bagh	Park	-	-	-	1	-	-	-	-
139.	Galiyara Parking Chowk	Parking	-	-	-	-	2	1	-	-
140.	Saragadi Parking (Below)	Parking	-	-	-	-	-	1	Yes	-
141.	Vijaynagar, Kashmir Avenue, Back side Krishna Sweets	Procession/ Gathering Hotspots	-	-	-	-	3	1	-	-
142.	Shivala Colony	Procession/ Gathering Hotspots	-	-	-	-	4	1	-	-
143.	Krishna Square, Water tank Park	Procession/ Gathering Hotspots	-	-	-	-	3	1	-	-
144.	Dumb School, Tehsilpura	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
145.	40 Kuh main park	Procession/ Gathering Hotspots	-	-	-	-	5	1	-	-
146.	Golden Avenue, Near Veer Heekikat Rai	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
147.	Focal point Opp. Police Station	Procession/ Gathering Hotspots	-	-	-	-	3	1	-	Yes
148.	Baba Deep Singh Nagar	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
149.	Veer Enclave, Opp. Riyan Public School	Procession/ Gathering Hotspots	-	-	-	-	4	1	-	-
150.	Hindu Sabha, Sr. Secondary School	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
151.	Park Shakti Nagar	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
152.	Subhash Park, Katra Sher Singh	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
153.	Town Hall	Procession/ Gathering Hotspots	-	-	-	-	3	1	-	-
154.	Ucha Park, Near GodamMohalla	Procession/ Gathering Hotspots	-	-	-	-	3	1	-	-
155.	Govt. Sr. Secondary School Gate, GT Road, Putiligarh	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
156.	Dhobi Ghat, Near Gate Hariman Chowk	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
157.	Friends Colony, Opp. Harimandir Majitha Road	Procession/ Gathering Hotspots	-	-	-	1	-	1	-	-
158.	Joshi Colony Park	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
159.	Park Pani wali Tanki, Near Japani Mill	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
160.	Triconi Park, Rani ka bagh	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
161.	Gurudwara Singh Sabha, Opp. Rani Ka Bagh	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-
162.	Goal Bagh	Procession/ Gathering Hotspots	-	-	-	-	2	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
163.	Railway station entry point	Railway Station Entry/Exit	1	1	-	-	-	-	-	-
164.	Railway station exit point	Railway Station Entry/Exit	1	1	-	-	-	-	-	-
165.	Railway station entry / exit, B/H	Railway Station Entry/Exit	2	2	-	-	-	-	-	-
166.	Railway station (In gate, towards platform)	Railway Station Entry/Exit	-	-	-	-	-	1	Yes	-
167.	Railway station (Out gate towards outside from the platform)	Railway Station Entry/Exit	-	-	-	-	-	1	Yes	-
168.	Railway station Parking lot	Railway Station Entry/Exit	-	-	-	-	-	1	Yes	-
169.	Domai Mandir	Religious place	-	-	-	-	3	-	-	-
170.	Gurudwara Shaheedan Sahib	Religious place	-	-	-	-	-	1	Yes	-
171.	B.K E&I Sr.Sec School	School	-	-	-	-	2	-	-	-
172.	B.K Dutt Gate	School	-	-	-	-	3	-	-	-
173.	Arya School Lohgarh	School	-	-	-	-	2	-	-	-
174.	DAV School both side Gate I/S	School	-	-	-	-	2	-	-	-
175.	DAV College Inside Both Outside	School	-	-	-	-	2	1	-	-
176.	DAV International School Bypass	School	-	-	-	1	-	-	-	-
177.	Jamunwali Road	School	-	-	-	-	2	-	-	-
178.	B.R Modern School	School	-	-	-	-	2	-	-	-
179.	DAV Police Public School	School	-	-	-	-	2	-	-	-
180.	Khalsa College Near Nikkasingh	School	-	-	-	-	2	1	-	-
181.	Metro Bus Stand Near Khalsa	School	-	-	-	1	-	-	-	-
182.	Govt. senior secondary school,	School	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
183.	Rashtriya Bal School Islamabad	School	-	-	-	-	2	-	-	-
184.	Model School Islamabad	School	-	-	-	-	2	-	-	-
185.	RBBSK Primary School	School	-	-	-	-	2	-	-	-
186.	Atom Public School Islamabad Chaatwali Gali	School	-	-	-	-	2	-	-	-
187.	Apex International School, Rani ka Bagh	School	-	-	-	-	2	-	-	-
188.	NavBharat School 33 Number	School	-	-	-	1	-	-	-	-
189.	Khalsa School	School	-	-	-	-	2	-	-	-
190.	Twinkle Star School Guru Nanak	School	-	-	-	-	2	-	-	-
191.	Bhavan SI Public School 33	School	-	-	-	-	2	-	-	-
192.	SSSS School	School	-	-	-	-	2	-	-	-
193.	Ram Ashram School	School	-	-	-	-	2	-	-	-
194.	Police DAV School Lawrence	School	-	-	-	-	2	-	-	-
195.	Guru Har Krishan Public School or CKD College GT Road	School	-	-	-	-	2	-	-	-
196.	Holi Heart School GT Road	School	-	-	-	-	2	-	-	-
197.	Prem Ashram School, Beri gate Market	School	-	-	-	-	2	-	-	-
198.	Hindu Sabha School	School	-	-	-	-	2	-	-	-
199.	Prakash Ashram School, Inside Hatti Gate	School	-	-	-	-	2	-	-	-
200.	Khalsa College Ranjit Avenue	School	-	-	-	-	2	-	-	-
201.	BBK DAV International School	School	-	-	-	-	2	-	-	-
202.	Ryan International	School	-	-	-	-	2	-	-	-
203.	DPS School	School	-	-	-	-	2	-	-	-
204.	Sant Kabir Public School Mandir Val Bazaar	School	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
205.	Ajit Vidhyalaya School Sultwind	School	-	-	-	-	2	-	-	-
206.	Shaheed Baba Pratap Sing	School	-	-	-	-	2	-	-	-
207.	Saint Joseph School Rani ka	School	-	-	-	-	2	-	-	-
208.	Saint Joseph School Fatahpur	School	-	-	-	-	2	-	-	-
209.	Cambridge School Loharka Road	School	-	-	-	-	3	-	-	-
210.	Meeri Peeri School	School	-	-	-	-	2	-	-	-
211.	Sacred Heart School Chungi	School	-	-	-	-	2	-	-	-
212.	SM High Scholl Vikas Nagar	School	-	-	-	-	2	-	-	-
213.	DD High School Gobind Pura	School	-	-	-	-	2	-	-	-
214.	Narangarh Govt. School Chehra	School	-	-	-	-	2	-	-	-
215.	Govt. School Nava Kot	School	-	-	-	-	2	-	-	-
216.	Amar School Nava Kot	School	-	-	-	-	2	-	-	-
217.	Twinkle Star School Navakot	School	-	-	-	-	2	-	-	-
218.	Hare Krishna Public School Majitha Road Bypass	School	-	-	-	-	2	-	-	-
219.	Spring Dale School	School	-	-	-	-	2	-	-	-
220.	Savan School Devi Nagar Fatehgarh Churian Road	School	-	-	-	-	2	-	-	-
221.	Shiv Deep Public School New Nehru Colony	School	-	-	-	-	2	-	-	-
222.	JK Public School Tung bala	School	-	-	-	-	2	-	-	-
223.	Govt. Public Tung Bala	School	-	-	-	-	2	-	-	-
224.	Model Study School Tung Bala Majitha Road	School	-	-	-	-	2	-	-	-
225.	Govt. Sr. Secondary School	School	-	-	-	-	2	-	-	-
226.	Preet Public School Mustafabad	School	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
227.	SS High School Tungbala Guru Gobind Sing Nagar	School	-	-	-	-	2	-	-	-
228.	Shivam Public School New	School	-	-	-	-	2	-	-	-
229.	Saranagdhar Sr. Secondary	School	-	-	-	-	2	-	-	-
230.	MahaShakti Vidhyabhawan Jawahar Road	School	-	-	-	-	2	-	-	-
231.	Bekish Shiksha Modern School Vijay Nagar	School	-	-	-	-	2	-	-	-
232.	Bright Way Public School	School	-	-	-	-	2	-	-	-
233.	Roaming Angels Public School	School	-	-	-	-	2	-	-	-
234.	Punjab High School Gali no 1	School	-	-	-	-	2	-	-	-
235.	Tagore Modern School	School	-	-	-	-	2	-	-	-
236.	Sham Public School Gali 3 Indra Colony Mustafabad	School	-	-	-	-	2	-	-	-
237.	Sunveli School Gopal Nagar Tower vali Gali	School	-	-	-	1	-	-	-	-
238.	GD Goenka School	School	-	-	-	-	2	-	-	-
239.	CLH School Islamabad Dargah	School	-	-	-	-	2	-	-	-
240.	CLH School Putligarh	School	-	-	-	-	2	-	-	-
241.	Ajanta Public School	School	-	-	-	-	2	-	-	-
242.	Bibek Academy School	School	-	-	-	-	2	-	-	-
243.	Govt. Sen. Sec School, Dhapai	School	-	-	-	-	2	-	-	-
244.	Government Girls Senior Secondary School, Sundar Gali Bahadur Nagar, Katra Ahluwalia	School	-	-	-	-	2	-	-	-
245.	Govt. Girls Higher Secondary School, M S Gate, Shivala Road Katra Bhagian, Hall Bazar	School	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
246.	Govt. high school, Rajinder Nagar Gali Number 3 Prem Nagar	School	-	-	-	-	2	-	-	-
247.	Government Middle School Railway B Block	School	-	-	-	-	2	-	-	-
248.	Government Senior Secondary School, GT Road Naraingarh, Azad Nagar	School	-	-	-	-	2	-	-	-
249.	Government High School, Karampura, E-Block	School	-	-	-	-	2	-	-	-
250.	Govt. High School, Kala Pind	School	-	-	-	-	2	-	-	-
251.	Government Girls High School, M.C.Market, Bhagta Wala Gate	School	-	-	-	-	2	-	-	-
252.	Government Saragarhi Memorial Secondary School	School	-	-	-	-	2	-	-	-
253.	Government Saragarhi Memorial Secondary School, High School	School	-	-	-	-	2	-	-	-
254.	Sarkari Secondary School, Katda Hakima, Outside Hakima Gate	School	-	-	-	-	2	-	-	-
255.	Vishav Public High School, Batala Rd, Guru Nanak Nagar	School	-	-	-	-	2	-	-	-
256.	Heritage walk	Tourist Hotspot	-	-	-	-	-	1	Yes	-
257.	Jamadar Haweli	Tourist Hotspot	-	-	-	-	3	-	-	-
258.	Pumme Di Pulli Near Bhadrakali	Tourist Hotspot	-	-	-	-	2	-	-	-
259.	Islamabad T-point to govindgarh	Tourist Hotspot	-	-	-	-	3	-	-	-
260.	Baba Shahib Chowk	Tourist Hotspots Entry/Exit Points	-	-	-	-	3	-	-	-
261.	Ramsar Road Near Baba Deep Singh Gurudhwara	Tourist Hotspots Entry/Exit Points	-	-	-	-	2	-	-	-
262.	Kichlu Chowk	Traffic Congestion Point	-	-	-	-	-	1	-	-
263.	Khajana Gate	Traffic Congestion Point	-	-	-	-	4	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
264.	Chabal Road mord gurbash nagger(Nr.Bhadrakali Mandir)	Traffic Congestion Point	-	-	-	-	4	-	-	-
265.	Bhandari Bridge	Traffic Congestion Point	-	-	-	-	4	1	-	-
266.	Hall Gate	Traffic Congestion Point	-	-	-	-	2	1	-	-
267.	Kairon Market	Traffic Congestion Point	-	-	-	-	2	-	-	-
268.	Kesar Da Dhaba	Traffic Congestion Point	-	-	-	-	2	-	-	-
269.	Islamabad Chowk	Traffic Congestion Point	-	-	-	-	2	-	-	-
270.	Income tax Chowk	Traffic Congestion Point	-	-	-	-	1	1	-	-
271.	Mall Cross Road	Traffic Congestion Point	-	-	-	-	1	-	-	-
272.	Novelty Chowk	Traffic Congestion Point	-	-	-	-	2	1	-	-
273.	Crystal Chowk	Traffic Congestion Point	-	-	-	-	2	2	Yes	-
274.	Tungawali Gali(ESI Road)	Traffic Congestion Point	-	-	-	-	2	-	-	-
275.	Borh wala Shivala batala road	Traffic Congestion Point	-	-	-	-	2	-	-	-
276.	Gumtala bypass chowk	Traffic Congestion Point	-	-	-	-	2	1	-	-
277.	Mustafa chowk	Traffic Congestion Point	-	-	-	-	2	-	-	-
278.	Green avenue park(Nr. verka booth)	Traffic Congestion Point	-	-	-	-	3	1	-	-
279.	Reyato chowk	Traffic Congestion Point	-	-	-	-	-	-	-	-
280.	Rattan Singh chowk	Traffic Congestion Point	-	-	-	-	-	-	-	-
281.	Verka bypass	Traffic Congestion Point	-	-	-	-	-	-	-	-
282.	Joshi colony market	Traffic Congestion Point	-	-	-	-	-	-	-	-
283.	District shopping centre	Traffic Congestion Point	-	-	-	-	-	-	-	-
284.	Masjid Bazarsirki Bandar	Traffic Junction	-	-	-	-	3	-	-	-
285.	Shakti Nagar Chowk	Traffic Junction	-	-	-	-	3	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
286.	Lahori gate	Traffic Junction	-	-	-	1	-	-	-	-
287.	Gate Hakima Main Chowk	Traffic Junction	-	-	-	-	3	-	-	-
288.	Chabal Road mord Gurbash	Traffic Junction	-	-	-	-	2	-	-	-
289.	T-Point Chabal Road	Traffic Junction	-	-	-	-	3	-	-	-
290.	Amritsar Entrance Bridge Nr.. Gurudhwara (gate Hakima)	Traffic Junction	-	-	-	-	3	-	-	-
291.	T-Point Mord Fatehsingh Colony	Traffic Junction	-	-	-	-	2	-	-	-
292.	Fatehsingh Colony Gali No:-22	Traffic Junction	-	-	-	-	3	-	-	-
293.	Husanpura circle	Traffic Junction	-	-	-	-	4	-	-	-
294.	Tandoor wala Chowk	Traffic Junction	-	-	-	-	5	-	-	-
295.	Sangam Chowk	Traffic Junction	-	-	-	-	4	1	-	-
296.	City Centre Market Front Side	Traffic Junction	-	-	-	-	2	1	-	-
297.	Surajchand Mansingh Gate	Traffic Junction	-	-	-	-	3	-	-	-
298.	Shera Wala Gate	Traffic Junction	-	-	-	-	3	-	-	-
299.	Ghee Mandi Akali Fhula Singh	Traffic Junction	-	-	-	-	2	-	-	-
300.	Chita Gummat Chowk	Traffic Junction	-	-	-	-	2	-	-	-
301.	Chimrang Road	Traffic Junction	-	-	-	-	3	-	-	-
302.	J.C Motor (100Ft Road)	Traffic Junction	-	-	-	-	3	-	-	-
303.	Mata Kola Chowk	Traffic Junction	-	-	-	-	4	-	-	-
304.	Pratap Nagar Near OBC Bank	Traffic Junction	-	-	-	-	2	-	-	-
305.	Thind Dairy	Traffic Junction	-	-	-	-	2	-	-	-
306.	New Amritsar Gate	Traffic Junction	-	-	-	-	2	-	-	-
307.	Golden Gate	Traffic Junction	-	-	-	-	2	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
308.	Uttamnagar Ganda nala Sultantwind chowk	Traffic Junction	-	-	-	-	2	-	-	-
309.	Sultanwind Gate	Traffic Junction	-	-	-	-	4	-	-	-
310.	Ajit Nagar Chowk(Dhingra)	Traffic Junction	-	-	-	-	4	-	-	-
311.	Dana Mandi	Traffic Junction	-	-	-	-	3	-	-	-
312.	Jwala Mohan Floor Mill	Traffic Junction	-	-	-	-	2	-	-	-
313.	Roop Nagar Main Road Near Lovely Chicken 1	Traffic Junction	-	-	-	-	3	-	-	-
314.	Roop Nagar Main Road Near Lovely Chicken 2	Traffic Junction	-	-	-	-	2	-	-	-
315.	Shiv Gali	Traffic Junction	-	-	-	-	2	-	-	-
316.	Mahajan Kulfi Wala	Traffic Junction	-	-	-	-	3	-	-	-
317.	Goal Hatti Chowk	Traffic Junction	-	-	-	-	2	-	-	-
318.	RS Tower Chowk	Traffic Junction	-	-	-	-	2	-	-	-
319.	Shastri Market Dena Bank	Traffic Junction	-	-	-	-	2	-	-	-
320.	State Bank Chowk	Traffic Junction	-	-	-	-	4	-	-	-
321.	Amrita Talkie Chowk	Traffic Junction	-	-	-	-	2	-	-	-
322.	Ghee Mandi Mohalla	Traffic Junction	-	-	-	-	2	-	-	-
323.	T-Point Tahil Shaheb Bazar	Traffic Junction	-	-	-	-	3	-	-	-
324.	Guru Ravidas Road Hall Gate	Traffic Junction	-	-	-	-	2	-	-	-
325.	T-Point New Town Hall	Traffic Junction	-	-	-	-	2	-	-	-
326.	Chowk Regent Cinema Lassiwala	Traffic Junction	-	-	-	1	-	-	-	-
327.	Chowk Bharwan Ka Dhaba	Traffic Junction	-	-	-	-	2	-	-	-
328.	Chowk Katra Jaimal Singh	Traffic Junction	-	-	-	-	2	-	-	-
329.	Telephone Exchange	Traffic Junction	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
330.	Karmon Diodhi Chowk	Traffic Junction	-	-	-	-	2	-	-	-
331.	Turn Point Pratap bazar	Traffic Junction	-	-	-	-	3	-	-	-
332.	Katra Ahluwalia Chowk	Traffic Junction	-	-	-	-	2	-	-	-
333.	Turn Point Guru bazar	Traffic Junction	-	-	-	-	3	-	-	-
334.	Subhash Juice Bar Sikndari Gate	Traffic Junction	-	-	-	-	2	-	-	-
335.	Bombay Wala Kua	Traffic Junction	-	-	-	-	3	-	-	-
336.	Gurudwara Lohgarh Sahib	Traffic Junction	-	-	-	-	2	-	-	-
337.	Chowk Farid Mathian Wala	Traffic Junction	-	-	-	-	2	-	-	-
338.	Chitra Taki Road	Traffic Junction	-	-	-	-	2	-	-	-
339.	Outside Ram Baug Church Road	Traffic Junction	-	-	-	-	2	-	-	-
340.	Katra Baghian Chowk	Traffic Junction	-	-	-	-	3	-	-	-
341.	Wallah Mandi Back Side	Traffic Junction	-	-	-	1	-	-	-	-
342.	Fatehgarh Sukur Chak Bypass	Traffic Junction	-	-	-	-	4	-	-	-
343.	Gurudhwara Kotha Shaheb	Traffic Junction	-	-	-	-	2	-	-	-
344.	Chowk Bille wala Mohkamura	Traffic Junction	-	-	-	1	-	-	-	-
345.	Chowk Vallah	Traffic Junction	-	-	-	-	4	1	-	-
346.	Opposite Apex Hospital	Traffic Junction	-	-	-	1	-	-	-	-
347.	Gurudhwara Wala Chowk	Traffic Junction	-	-	-	1	-	-	-	-
348.	Pawan Nagar Gali No:-5	Traffic Junction	-	-	-	1	-	-	-	-
349.	Outside Jagat Jyoti School	Traffic Junction	-	-	-	-	2	-	-	-
350.	Chungjiyan Chowk	Traffic Junction	-	-	-	1	-	-	-	-
351.	Suncity T-Point & Suncity Mord	Traffic Junction	-	-	-	1	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
352.	Gurudwara Wali Gali:14 Dashmesh Nagar	Traffic Junction	-	-	-	1	-	-	-	-
353.	Chowk Judge Nagar (Nr.Gurudhwara Shahib)	Traffic Junction	-	-	-	-	2	-	-	-
354.	Matakola Balai Kendra Gali	Traffic Junction	-	-	-	-	2	-	-	-
355.	Outside Mission Compound	Traffic Junction	-	-	-	-	1	-	-	-
356.	Shivala Virbhan	Traffic Junction	-	-	-	-	2	-	-	-
357.	T-Point Ramanand Bagh	Traffic Junction	-	-	-	1	-	-	-	-
358.	Katra Karam Singh Chowk	Traffic Junction	-	-	-	-	2	-	-	-
359.	Purani Lakad Mandi Chowk	Traffic Junction	-	-	-	1	-	-	-	-
360.	Chowk Chabutra	Traffic Junction	-	-	-	-	2	-	-	-
361.	Sharma Colony Near	Traffic Junction	-	-	-	-	2	-	-	-
362.	Tapai Fatak	Traffic Junction	-	-	-	-	2	-	-	-
363.	Bakarmandi Chowk	Traffic Junction	-	-	-	1	-	-	-	-
364.	Chatiwind Chowk	Traffic Junction	-	-	-	-	4	2	-	-
365.	Chatikhui Chowk	Traffic Junction	-	-	-	-	2	-	-	-
366.	Purani Chungi Teg Royal Hotel Tarang Taran Road	Traffic Junction	-	-	-	-	2	-	-	-
367.	Maijivadiya Kabra	Traffic Junction	-	-	-	-	2	-	-	-
368.	Mohni Chowk	Traffic Junction	-	-	-	-	2	-	-	-
369.	Karori Chowk	Traffic Junction	-	-	-	-	2	-	-	-
370.	Laxmansar Chowk	Traffic Junction	-	-	-	-	2	-	-	-
371.	Chowk Gujjarpura	Traffic Junction	-	-	-	-	2	-	-	-
372.	Navacoat bazar Road	Traffic Junction	-	-	-	1	-	-	-	-
373.	T-point Right Bridge Near CKD	Traffic Junction	-	-	-	1	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
374.	B-Block gate 1,2	Traffic Junction	-	-	-	-	2	-	-	-
375.	Machi Mandi near Fatak	Traffic Junction	-	-	-	-	2	-	-	-
376.	Islamabad Bridge	Traffic Junction	-	-	-	1	-	1	Yes	-
377.	Soorchowk Balmiki CHowk	Traffic Junction	-	-	-	1	-	-	-	-
378.	Kishan Kot Fatak	Traffic Junction	-	-	-	-	2	-	-	-
379.	Bhagta wala gate	Traffic Junction	-	-	-	-	2	-	-	-
380.	Galwali gate	Traffic Junction	-	-	-	-	2	-	-	-
381.	Kallu ka akhada	Traffic Junction	-	-	-	-	2	-	-	-
382.	Naiya wala more	Traffic Junction	-	-	-	1	-	-	-	-
383.	Amritsar Improvement trust	Traffic Junction	-	-	-	-	1	-	-	-
384.	Ranjit Avenue T-Point	Traffic Junction	-	-	-	1	-	-	-	-
385.	Purani Chungi	Traffic Junction	-	-	-	1	-	-	-	-
386.	DC Kothi Green Avenue	Traffic Junction	-	-	-	1	-	-	-	-
387.	Joshi Colony Chowk	Traffic Junction	-	-	-	-	2	-	-	-
388.	Garden Colony	Traffic Junction	-	-	-	1	-	-	-	-
389.	Mord Guru Arjan Dev Nagar	Traffic Junction	-	-	-	-	2	-	-	-
390.	22 No Fatak	Traffic Junction	-	-	-	1	-	-	-	-
391.	Purani Chungi Chehrt Road	Traffic Junction	-	-	-	-	4	1	-	-
392.	Khandwala Near Chehta Road	Traffic Junction	-	-	-	1	-	-	-	-
393.	Sandhu Colony	Traffic Junction	-	-	-	1	-	-	-	-
394.	Kale Ka Mode Chehta Road	Traffic Junction	-	-	-	-	2	1	-	-
395.	Chehta Cross Road	Traffic Junction	-	-	-	1	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
396.	Narayan Garh Chehta	Traffic Junction	-	-	-	-	2	-	-	-
397.	Wadali T-Point	Traffic Junction	-	-	-	-	3	-	-	-
398.	Kort Khalsa CHowk	Traffic Junction	-	-	-	-	3	-	-	-
399.	Nika Singh Colony	Traffic Junction	-	-	-	-	2	-	-	-
400.	Darshan Singh Ka Dera	Traffic Junction	-	-	-	1	-	-	-	-
401.	Gawal Mandi Chowk	Traffic Junction	-	-	-	-	2	-	-	-
402.	Pipli Shab Gurudhwara	Traffic Junction	-	-	-	-	2	-	-	-
403.	Parshuram Chowk	Traffic Junction	-	-	-	1	-	-	-	-
404.	Bhandari Bridge To Goal Bagh (Pakode wala)	Traffic Junction	-	-	-	-	2	-	-	-
405.	UCO Bank	Traffic Junction	-	-	-	-	1	-	-	-
406.	Coat Atmaram Road	Traffic Junction	-	-	-	1	-	-	-	-
407.	Jaspal nagger DI Galiya	Traffic Junction	-	-	-	1	-	-	-	-
408.	Tej Nagar Chowk	Traffic Junction	-	-	-	-	2	-	-	-
409.	Chowk Tandan Nagar	Traffic Junction	-	-	-	1	-	-	-	-
410.	Murgikhane Wali Gali	Traffic Junction	-	-	-	-	2	-	-	-
411.	Banke bihari Wali Gali	Traffic Junction	-	-	-	1	-	-	-	-
412.	Baba Meer Shah Nehru Colony	Traffic Junction	-	-	-	-	3	-	-	-
413.	Papa public school, 88 feet road	Traffic Junction	-	-	-	-	2	-	-	-
414.	27ft Road Green Field Road	Traffic Junction	-	-	-	-	2	-	-	-
415.	Mai bhago college Majitha road	Traffic Junction	-	-	-	-	3	1	-	-
416.	D.R enclave	Traffic Junction	-	-	-	-	2	-	-	-
417.	Loharka chowk bridge	Traffic Junction	-	-	-	-	2	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
418.	Meera kot chowk	Traffic Junction	-	-	-	1	1	1	-	Yes
419.	Ekam Dhaba g.t road	Traffic Junction	-	-	-	-	2	-	-	-
420.	Pind heir	Traffic Junction	-	-	-	-	2	-	-	-
421.	Akash amar Chowk Fateh garh Chudiya Road	Traffic Junction	-	-	-	1	-	-	-	-
422.	Ajay Sr. Secondary School (Amar Jyoti School) Sakhe Di Haweli	Traffic Junction	-	-	-	-	2	-	-	-
423.	Fatehgarh Bypass Chowk	Traffic Junction	-	-	-	-	1	-	-	-
424.	Baba Deep Singh Colony	Traffic Junction	-	-	-	1	-	-	-	-
425.	Govt. High school near park pani wali tenka friends colony	Traffic Junction	-	-	-	-	2	-	-	-
426.	Civil line T-Point Near Namthari Gurudhwara	Traffic Junction	-	-	-	1	-	-	-	-
427.	Hukumsingh Road	Traffic Junction	-	-	-	1	-	-	-	-
428.	Company Baug	Traffic Junction	-	-	-	-	2	-	-	-
429.	Congress bhavan, Near Circuit House	Traffic Junction	-	-	-	-	3	-	-	-
430.	Doaba Chowk	Traffic Junction	-	-	-	-	3	-	-	-
431.	Daily Needs	Traffic Junction	-	-	-	-	2	-	-	-
432.	Guru Arjun Dev Nagar Mod	Traffic Junction	-	-	-	-	2	-	-	-
433.	Gopal Mandir Chowk	Traffic Junction	-	-	-	-	3	1	-	-
434.	Jaliawala Baug	Traffic Junction	-	-	-	-	2	-	-	-
435.	Amritbakery Opp.-Kabir Park	Traffic Junction	-	-	-	-	2	-	-	-
436.	Kabir Park Market Opp.-GNDU	Traffic Junction	-	-	-	-	2	1	-	-
437.	Shivaji Park, Rani ka Bagh	Traffic Junction	-	-	-	-	3	1	-	-
438.	Katra Moti Ram park Near Soyabin Wali Dukan	Traffic Junction	-	-	-	-	3	1	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
439.	Park Beri gate	Traffic Junction	-	-	-	-	2	1	-	-
440.	Isvar nagger Chawk	Traffic Junction	-	-	-	1	-	-	-	-
441.	Guru Amar Das Nagar Chawk	Traffic Junction	-	-	-	1	-	-	-	-
442.	Bagchi lakha Singh Chawk	Traffic Junction	-	-	-	1	-	-	-	-
443.	Guru Nanak Nagar, Street No. 1	Traffic Junction	-	-	-	-	4	1	-	-
444.	Chotta Haripur Chawk	Traffic Junction	-	-	-	-	4	1	-	-
445.	Mahakali Nav Greh Mandir, Shastri Nagar	Traffic Junction	-	-	-	1	-	-	-	-
446.	Basant Avenue Market	Traffic Junction	-	-	-	-	-	-	-	-
447.	Lawrence cross road	Traffic Junction	-	-	-	-	-	-	-	-
448.	DAV college / Lawrence road	Traffic Junction	-	-	-	-	-	-	-	-
449.	Dausanda Singh chowk	Traffic Junction	-	-	-	-	-	-	-	-
450.	Trillium mall junction	Traffic Junction	-	-	-	-	-	-	-	-
451.	ESI cross road	Traffic Junction	-	-	-	-	-	-	-	-
452.	88 ft. Road entry	Traffic Junction	-	-	-	-	-	-	-	-
453.	88FT exit	Traffic Junction	-	-	-	-	-	-	-	-
454.	Kabir Marg	Traffic Junction	-	-	-	-	-	-	-	-
455.	Makhan Restaurant chowk	Traffic Junction	-	-	-	-	-	1	Yes	-
456.	SSSS chowk	Traffic Junction	-	-	-	-	-	-	-	-
457.	Circular road (opposite TSPCL)	Traffic Junction	-	-	-	-	-	-	-	-
458.	Musta chowk (Bagh chowk)	Traffic Junction	-	-	-	-	-	-	-	-
459.	Gala Mala Marg	Traffic Junction	-	-	-	-	-	-	-	-
460.	C Block market	Traffic Junction	-	-	-	-	-	-	-	-

S.No	Area of the City	Category	ANPR	Indoor FRS	Outdoor FRS	360°	Fixed	PTZ	PAS	ECB
461.	Green Avenue market	Traffic Junction	-	-	-	-	-	-	-	-
462.	Amrit nal bagh	Traffic Junction	-	-	-	-	-	-	-	-
463.	Durgiyana Mandir (Hathi chowk)	Traffic Junction	-	-	-	-	-	1	Yes	-
464.	Durgiyana New Entrance	Traffic Junction	-	-	-	-	-	-	-	-
465.	Sultan Wind 100 feet road	Traffic Junction	-	-	-	-	3	1	-	-
466.	Gurunam nagger	Traffic Junction	-	-	-	-	2	1	-	-
		TOTAL	72	21	35	78	778	129	25	10

9 Appendix VI: Air Quality Monitoring Station Locations

S. No.	Location Details	Quantity
1.	Batala Road – Old Focal Point	1
2.	Ranjit Avenue Market	1
3.	Amritsar Bus Stand	1
4.	Sultan Wind Clothes Market	1
5.	East Mohan Nagar	1
6.	Tarn Taran Road	1
7.	Jambia	1

10 Appendix VII: Water Quality Analyzer Locations

S. No.	Name of the Location	Quantity
1.	Tung Dhab Drain	1
2.	City Outfall Drain	1
3.	Tarowali Head Works	1

11 Appendix VIII: Indicative Use Cases

S. No.	Functionality	Detailed Use Case
1.	Camera Blocked	<ul style="list-style-type: none"> The Video Analytics System should have the capability to generate the alert in case any object has blocked its lenses.
2.	Camera Tampering	<ul style="list-style-type: none"> The VA System should have the capability to generate the alert in case the camera has been tampered by way of change of Field of view of camera, blurring of view, blocking of view by cloth or obstruction, camera disconnection, blinding of camera by laser or flashlights
3.	Camera FOV Change	<ul style="list-style-type: none"> The VA System should have the capability to generate the alert in case the Field of View (FoV) of the camera changes.
4.	Video Analytics with PTZ cameras	<ul style="list-style-type: none"> The VA System should have the capability to recognize and track the person / object in the field of view with PTZ cameras, Alarm object tracking from fix camera to PTZ camera, Alarm object tracking from PTZ camera to PTZ camera and Object tracking underneath the camera
5.	Un-attended object search	<ul style="list-style-type: none"> The VA System should have the capability to detect an unattended object in the camera field of view. The VA should be intelligent to understand the existing objects within the camera field of view and should generate an alert only when a new object is detected for more than the preconfigured duration of time. The existing objects should be learnt by the system based on the training of the system. The VA should generate an alert in such an instance with the evidence video. It shall be possible to search exact moment when an unattended object was left at that spot and trace the person who left it using Person of Interest search.
6.	Person of Interest Search	<ul style="list-style-type: none"> The VA System should have the capability to search people based on the attributes such as type of dress (to include common Indian dressing styles along with colour of the clothes), height, skin colour, body build etc. It shall be possible to search the suspect or identify his last known location or current location based on video camera footage.
7.	Crowd Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect the crowd formation in any part of the scene based on the threshold value of number of persons based on the user selection. The VA System should also estimate the number of persons in the crowd and should raise an alert with the estimated number of persons.
8.	Person Collapsing Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect the person collapsing suddenly in the camera field of view. The VA should generate an alert in such a situation with the evidence video.

S. No.	Functionality	Detailed Use Case
9.	Fire Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect fire anywhere in the camera field of view for more than the preconfigured duration. The VA should generate an alert with evidence video
10.	Smoke Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect medium or high-density smoke anywhere in the camera field of view for more than the preconfigured duration. The VA should generate an alert with the evidence video.
11.	Traffic Congestion Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect the vehicle which stops in a patch of the road and halts more than the user configurable duration. The VA should raise an alert in such a situation. The VA should have the capability to detect the congestion on the road due to vehicle pile-up.
12.	Wrong Direction Traffic Flow	<ul style="list-style-type: none"> The VA System should have the capability to detect the vehicle moving in the wrong way for the configured patch of the road. The VA System should raise an alert in such a situation.
13.	Parking Violation Detection	<ul style="list-style-type: none"> The VA System should have the capability to detect the vehicle stopped on the road in the no parking zone more than the user configured duration. The VA System should raise an alert in such a situation.
14.	Vehicle Colour Search	<ul style="list-style-type: none"> The VA System should have the capability to detect the colour of the vehicle during the day light and should offer the facility to search the vehicles based on the vehicle colour.
15.	Perimeter Protection	<ul style="list-style-type: none"> The VA System should have the capability to detect the person trying to jump the perimeter or cross virtual tripwire between specified times of the day.
16.	Loitering	<ul style="list-style-type: none"> The VA System should have the capability to detect loitering incidents in crime hotspot areas.
17.	Red Light Violation Detection	<ul style="list-style-type: none"> The VA System shall have capability for Red Light Violation detection for cameras installed on traffic junctions.
18.	Identification of Abandoned objects and generation of alarm thereof	<ul style="list-style-type: none"> Surveillance cameras continuously monitor and run the configuration to identify the abandoned objects in its vicinity If an abandoned object is identified an alert is generated The alert is displayed on the control centre dashboard with required details like location etc. The alert is used to activate other cameras to record activities at the same location When an object is identified by video analytics, video management server will identify the time line and record the video feed at the command centre for the time The alert can also be sent to other cameras in the vicinity for additional video feeds around the incident Surveillance operator and analytics expert run through the video feed and identify the suspect

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • The SOP is run by surveillance operator to create a service assignment to the police station • All the images and videos are sent along with the details to the police as part of the SOP • All the details including photo of the culprit will be multi cast across the mobile surveillance vehicles and other police officials • Incident is tracked and updated to closure
19.	Making way to Emergency vehicles/Ambulances	<ul style="list-style-type: none"> • Availability of Ambulance, Location of Ambulance, Location of hospitals on GIS Map, Operator aware of type of mishap to dispatch to relevant hospital or as per patient attendant request, Police personals deployed at each location in the city and their contact information, communication channel, Command control traffic controller • Incident details received from the location to control centre • Help desk analyses the situation and figure out SOP Operator to follow SOP defined as per trigger and co-ordinate with ambulance, Traffic police, City police through SOP • Incident data is created automatically and/or manually regarding the emergency while running the SOP • Dispatch an Ambulance, Police, display information on VMS regarding emergency to citizens and request to make way for Ambulance • All the respective team's co-ordinate and help ambulance pick the patient • Emergency operator analyses & share faster route for the ambulance to reach to the patient and back to the hospital • Change switching cycles of traffic signals • Incident is updated with all relevant details.
20.	Controlling Multiple Cameras using PTZ joystick	<ul style="list-style-type: none"> • Live video streaming is available on the video wall from PTZ cameras. The users can monitor: <ul style="list-style-type: none"> ○ Live video streaming of locations across the city using PTZ cameras ○ PTZ cameras to zoom and tilt to focus on locations of incidents that help recognize the suspect.
21.	Face Recognition System (FRS)	<ul style="list-style-type: none"> • Face Recognition cameras shall be Full HD (1920 X 1080) @ 30 FPS and shall be installed at transit hubs like Airports, Railway Stations and Bus Stands at building entry and exit gates (indoor environment). These shall also be installed at crime hotspots in the city in an outdoor environment

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • These cameras shall be mounted at a height of approximately 5-10 feet to capture faces clearly at distance of up to 3 meters • The face recognition cameras shall transmit maximum resolution uncompressed video feed for best face recognition results to Local Processing Unit (LPU) inside junction boxes for processing and extracting face recognition minutiae from the video feed. Only minutiae shall be shared with Face Recognition head end software at the ICCC for further matching and alert generation Alternatively, video streams can also be analysed at server end without local processing unit • The face recognition cameras shall send a compressed video stream to ICCC for video recording and analytics for evidence purpose and general surveillance • The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system • The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator • The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real-time report such as Audit log report, Hit List Report, Daily Statistics Report, and Distribution Report • The facial recognition system should be accessible from 5 different desktop/laptops at any given time. When choosing a distributed architecture, the system shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision • The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts • The algorithm for facial recognition or the forensic tool should be able to recognize partial faces with varying angles

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • The system should be able to detect multiple faces from live single video feed • The system should have combination of eye-zone extraction and facial recognition • The system should have short processing time and high recognition rate • The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions) • Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall use of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments • The system should be able to identify and authenticate based on individual facial features • The system should be compatible with the video management system being proposed by the system integrator • The system should have capability for 1:1 verification and 1: N identification matching • The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc. • The system should be able to support diverse industry standard graphic and video formats as well as live cameras • The system should be able to match faces from recorded media • The system should be able to detect a face from a group photo • The system should be able to detect a face from stored videos of any format • The system should have bulk process of adding faces in the system • The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing • The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for windows OS or android OS to capture a face on the field and get the matching result from the backend server

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas • The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted" • It should be able to provide information such as Gender & Age Group along with facial detection/match data <p>Face Recognition System (FRS) is designed for identifying or verifying a person from various kinds of photo inputs from digital image file to video source. The system should offer logical algorithms and user-friendly, simple graphical user interface making it easy to perform the facial matching.</p> <p>The system can be able to broadly match a suspect/criminal photograph with database created using photograph images available with Passport, CCTNS, and Prisons, State or National Automated Fingerprint Identification System or any other image database available with police/ other agencies. The system can be able to:</p> <ul style="list-style-type: none"> • Capture face images from IP Camera feed and generate alerts if a blacklist match is found. • Search photographs from the database matching suspect features • Matching suspected criminal face from pre-recorded video feeds obtained from IP cameras deployed in various critical identified locations, or with the video feeds received from private or other public organization's video feeds • Adding photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches • Investigate to check the identity of individuals upon receiving such requests from Police Stations
22.	Automatic Number Plate Recognition (ANPR)	<ul style="list-style-type: none"> • The ANPR System should be capable of detecting and converting vehicle license plates into English readable OCR data. The system should support real-time detection of vehicles at the deployed locations, recording each four wheelers, 2 wheelers and other vehicle type 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 should be privilege driven using password authentication for VMS GUI access

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • ANPR cameras shall be mounted at City Entry/Exit Points and at Transit Hubs like Railway Stations, Bus stands and Airports primarily for purpose of surveillance only. The system shall have capability to compare license plates against a blacklisted or stolen vehicle database that is part of the system for alert generation • It shall be possible to get all real-time alerts on a city map at ICC, related to location of detection of blacklisted vehicle with all extracted data characteristics of the vehicle including speed • The system shall also show location of all existing Dispatch Units on a map to know which one is closest to the location • The system shall have capability to integrate with an external Computer Aided Dispatch (CAD) system via API and the MSI shall be responsible to make this integration to trigger automatic incident creation and dispatch on detection of the blacklisted vehicles • The system shall have capability to queue all pending incidents (of detection of blacklisted vehicles) so that CAD operators can attend to them one by one. • The system shall maintain complete record of all vehicles detected in an audit trail for record keeping and audit purpose • ANPR cameras shall be required to work at 30 FPS at Full HD (1920 X 1080) resolution with 5 to 50 mm lens high quality lens. • The ANPR cameras can transmit uncompressed video feeds for better accuracy to Local Processing Units (LPU) inside the junction boxes for extracting <ul style="list-style-type: none"> a. Vehicle Number Plate b. Other characteristics like vehicle colour, type, count etc. using Automatics Traffic Counter Classifier (ATCC) function c. Speed of the vehicle • A single compressed stream shall also be sent to server for recording and general video analytics purpose • The LPU shall transfer the extracted metadata with cropped license plate images to the ANPR head end software for further processing and alerts generation. • At the City Entry/Exit points they shall be required to be mounted on a cantilever pole arm with each ANPR camera covering one lane. The height of installation shall be approximately 6 meters

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • At the transit hub they shall be mounted at entry and exit gates and installed to cover all vehicles that enter and exit these locations • Vehicle Detection and Video Capture Module <ul style="list-style-type: none"> a. The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition. • License Plate Detection <ul style="list-style-type: none"> a. The System shall automatically detect the license plate in the captured video feed in real-time. b. The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts). c. The System shall store JPEG image of vehicle and license plate and enter the license plate number into database along with date time stamp and site location details. d. System should be able to detect and recognize the English alpha numeric License plate in standard fonts and formats of all vehicles including cars, HCV, and LCV. e. The system should be able to process and read number plates of vehicles with speed of up to 200 km/hr. f. The system shall be robust to variation in License Plates in terms of font, size, contrast and colour and should work with good accuracy. • Colour Detection <ul style="list-style-type: none"> a. The system shall detect the colour of all vehicles in the camera view during daytime and label them as per the predefined list of configured system colours. The system shall store the colour information of each vehicle along with the license plate information for each transaction in the database b. The system shall have options to search historical records for post event analysis by the vehicle colour or the vehicle colour with license plate and date time combinations • Alert Generation <ul style="list-style-type: none"> a. The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel b. The system should be able 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 • Vehicle Log

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> a. Vehicle Make Detection Module The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. b. The system should provide advanced and smart searching facility of License Plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1 and 2-character distance) • Vehicle Make Detection Module <ul style="list-style-type: none"> a. System should be able to identify the make of the vehicle coming in the field of view of the camera with good accuracy • Vehicle Classification module <ul style="list-style-type: none"> a. System should be able to classify the vehicle into LMV, H MV and 2-wheelers • Over Speed Detection Module: <ul style="list-style-type: none"> a. The system should be able to detect vehicles moving up to speeds of 200 km/hr. and read their number plates with good accuracy. Vendor should provide manufacturer certificate/test report in support of their claim b. The certification for the accuracy of speed measurement should be from the approved Govt. body from the country of origin. Certifications shall be provided for the complete system and not individual components. The system should be calibrated for accuracy prior to handing over and the successful bidder should ensure annual calibration of the system • Central Management <ul style="list-style-type: none"> a. The Central Management Module shall run on the ANPRS Central Server at ICCC. It should be possible to view records and edit hotlists from the Central Server • The system should be able to do - No helmet detection for 2-wheelers • The system should have reading accuracy of 80% on vehicles including 2 & 4 wheelers which are visible by human eye for English alphanumeric number plates excluding cursive fonts
23.	Emergency Call Box (ECB) with Panic Button	<ul style="list-style-type: none"> • ECB with panic button shall help citizens/visitors/tourists report the distress conditions related to law and order incidents or traffic incidents or other emergencies • The emergency call box will enable citizens to establish a two-way audio (microphone and speaker) & camera (video camera and a video screen) communication link with ICCC personnel through a press of a button.

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> Multiple SOPs are preconfigured for different incidents like medical emergency, accidents, terrorist, eve-teasing, waterlogging, fire, earthquakes, bomb threat, public disturbances etc.
24.	Integration of ICCC with Dial 112 project.	<ul style="list-style-type: none"> The ECB shall be integrated with the centralized Dial 112 project planned at the state level for escalating all the incidents detected from video surveillance in the city. The envisaged ICCC under smart city shall have the facility of the dispatch centre. The following are the envisaged activities <ol style="list-style-type: none"> MSI shall be responsible to integrate centralised call taker centre Dial 112 and vehicle dispatch centre with ICCC MSI shall be able to create incidents in the Dial 112 web based portal based on the alerts generated in the surveillance system MSI should be able to dispatch/communicate with the required police, fire and ambulance vehicle covered in the dial 112 system MSI shall be able to update the created incidents, update incidents and close the incidents based on the alerts generated by the surveillance system MSI shall be able to make out bound calls to the dispatch vehicles MSI shall develop APIs of the Surveillance system which should be seamlessly integrated with the dial 112 for generation of the incidents. MSI shall be responsible to generate display whenever there is an incident and the respective camera video should be played in the screen
25.	ICCC Platform: Disaster management & emergency incident management	<ul style="list-style-type: none"> Provide seamless incident–response management, collaboration and geo-spatial display. Provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Provide Standard Operating Procedures (SOPs), step-by-step instructions based on the Authorities policies and tools to resolve the situation and presents the relevant situation information in a quick and easily digestible format for an operator to verify the situation. Shall be a combination of key functionalities like Data Normalization, IoT Platform, API Manager/Gateway, Database and ICCC application

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> Proposed Solution architecture should have combination of data normalization (IoT Platform) and City operation centre software functionalities covering Complex Event Processing, Rules Engine, Map and Video Based Visualization.
26.	ICCC Platform: Controlling and monitoring of civic amenities	<ul style="list-style-type: none"> Integration of field devices (Street light controllers, GPS Tracking of Vehicles, RFID Bins, Water SCADA, Air Sensors, Water Sensors), Mapping of available parking lots with ICCC Platform
27.	Single Dashboard for Operations and integration of Dashboard with all smart ICT solutions	<ul style="list-style-type: none"> Single Dashboard for Operations shall provide Information to department which will help in Project Monitoring and coordination amongst Departments. Integration of dashboard with field devices with ICCC Platform I.e. Street light controllers, GPS Tracking of Vehicles, RFID Bins, Water SCADA, Parking sensors.
28.	Intelligent Street Lighting System	<ul style="list-style-type: none"> Intelligent Street Lighting System shall be used to optimise the electricity consumption by switching ON and OFF the lights of a switching point and/or networked switching points from ICCC instantaneously or automatically throughout the year on basis of Sunrise and Sunset time depending on the geographical location of the switching point Enabling city to generate information about its own lighting infrastructure (usage, maintenance and alert conditions) Control of power theft from street lighting network
29.	Public Address System	<ul style="list-style-type: none"> Public address system can be used to address the people in case of situations like public disturbances at a location. This PAS system can be used in conjunction with the surveillance cameras installed at the locations. The IP based PAS systems can also be used to broadcast general and emergency messages for public awareness. Address and announcement of voice messages for Public on road, tourist places and other traffic junctions. Use public announcement system to make important and relevant announcements
30.	Variable Message Displays: notifications	<ul style="list-style-type: none"> Variable Message Display board is used for showing emergency/disaster related messages as and when required. The information provided through VMD in urban areas includes traffic congestion, accidents and incidents notification, alternate routes, weather condition, road work zones and speed restrictions etc. The objectives of Variable Message Display are: <ol style="list-style-type: none"> To provide real-time information on the state of the network to drivers. To improve road safety by providing updates regarding accidents, adverse weather and road works.

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> c. To intimate drivers about changes in number of lanes, speed limits etc. d. Environmental aspects including Air pollution, weather condition etc.
31.	Variable Message Displays: Revenue Generation By advertisements	<ul style="list-style-type: none"> • Variable Message Display (VMD) boards can be used for advertisements for generation of revenue. • Automatic display of pre-defined messages based on rules (such as time of the day, event, traffic congestion etc.) • Operator can shall schedule a message to be displayed at specific intervals or configure to display dynamic information on regular basis.
32.	Air Quality Monitoring System: Real-time City Data Monitoring & Notifications	<ul style="list-style-type: none"> • The environmental monitoring solutions are installed across to city and data is collected for hazardous gases like SoX, NoX, and CoX. The data collected over a period is used for analysis. • Air Quality Analyser monitor the air quality and transmit data to the Command and Control Centre at pre-defined time interval • Real-time data shall be analysed, presented on dashboard with alerts • The outcome of data analytics in the form of reports shall provide the trend in increasing/decreasing pollution levels across the city. This data shall be shared with pollution control board to take corrective measures to control the pollutants. The pollution board shall look at development of standards and guidelines for industry specific emissions and effluents standards, Training, Pollution control technology, Pollution control enforcement, Mass awareness and publications etc. • Sharing the information on pollution, temperature & humidity data to citizens using application and VMD • Municipal officials will have access to separate data points for various areas in Amritsar. This data could help officials analyse and compare pollution data to plan for future pollution management initiatives across city. • Central Air Quality Monitoring Software collect data over a period to generate trend analysis on pollution levels in the City • Central control system shall capture and display/ provide feed on the air quality parameters at website / portal / mobile application • The collated environmental information shall be relayed instantaneously to local Variable Messaging Sign Boards (Vamps) mounted on poles alongside the Air Quality Monitoring Stations • The Air Quality Monitoring system shall also be integrated with the state and central pollution control board website and database via API integration to share data with them on regular intervals

S. No.	Functionality	Detailed Use Case
		<ul style="list-style-type: none"> • Punjab Pollution Control board takes mitigation action on the Air Pollution. • The collated environmental information shall be relayed instantaneously to local Variable Messaging Sign Boards (Vamps) mounted on poles alongside the Air Quality Monitoring Stations • The outcomes can be shared via SMS during extreme conditions with citizens
33.	Waste Water Quality Monitoring System: Monitoring & Notifications	<ul style="list-style-type: none"> • Water Quality Management System (OWQMS) to monitor the quality of waste-water in the drainage canals and monitor effluent treatment measures being done in the canal. • Primary objective of the Online Water Quality Management System (OWQMS) for drainage canals in Amritsar city under the smart city program is to monitor the quality of waste-water in the drainage canals and monitor effluent treatment measures being done in the canal. The project goals shall be to provide the following: <ol style="list-style-type: none"> a. Monitoring of drainage water quality from ICC b. Monitoring the Quality of effluent treated and processing at the inlet and discharge of each drain (Tung Dhab and City Outfall) c. Measure waste water quality parameters like BOD, COD, Dissolved Oxygen, TSS, NH4-N, PH, Temperature and Oil & Grease in Tung Dhab and City Outfall Drain d. Integrate data with State and Central Pollution control websites and databases. e. Punjab Pollution Control board shall utilize real-time water quality parameters collected from quality sensors across the drainage canals to analyse and detect waste water quality anomalies.

13 Appendix X: Existing city surveillance infrastructure

Existing CCTV Infrastructure

S. No.	Product Description	Make and Model	Quantity (Nos.)
1.	Fixed Camera 2 MP	Axis M1125-E	120
2.	Fixed Camera 1 MP	Axis M1124-E	80
3.	PTZ Camera 2 MP	Axis P56	2
4.	Services Machine with Windows Server 2012 64 bits R2 OS	Lenovo RD450 with Windows Server 2012 64 bits R2 OS	6
5.	Video Management Software Base License with SMA STANDARD Licenses	Genetics (GSC-Om-S) including SMA	6
6.	Video Management Camera license	Genetics (GSC-Om-S-1C)	202
7.	4TB HDD	Lenovo	42
8.	HDMI Cable	Standard	6
9.	22" Desktop Monitors	LG 22MP58	6
10.	24U Server Rack	Schneider	6
11.	2 KVA online UPS	Eaton 2000INXL	6
12.	Outdoor Junction Box – Metal	Rittal AE 1350.500	40
13.	Outdoor Junction box – Fiber	SIntex 4030	40
14.	Voltage Stabilizers	Accurate 1000VA	40
15.	Outdoor Network Cable Cat 6	DIGILINK	15000
16.	Power cable	Polycab	5000
17.	24 port loaded Patch Panel	DIGILINK	6
18.	Cat 6 Patch Cord 1 Meters.	DIGILINK	60
19.	Cat 6 Patch Cord 1 Meters.	DIGILINK	30
20.	Core Switch	Netgear GS724T	6
21.	Field Switches	Netgear GS110TP	41
22.	Tower for mounting Wireless Equipment	Fabricated	6
23.	6 m Poles	Fabricated	40
24.	Wireless Access points Radios	UBNT R5AC-PTMP	12
25.	Access Points Antennas	UBNT AM-5AC21-60	12
26.	Wireless Radios	UBNT PBE-5AC-500	55

Existing Surveillance Camera Location Details

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
1.	Lawrence Road Police Chowki	Basant Avenue Market	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
2.		Income Tax Chowk	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
3.		Rialto Chowk	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
4.		Lawrence cross Road	6	1	-	-
				1	-	-
	1			-	-	
	1			-	-	
	1			-	-	
	1			-	-	
5.	DAV College / Lawrence Road	3	1	-	-	
			1	-	-	
			1	-	-	
6.	Purani Chungi	5	-	1	-	
			-	1	-	
			-	1	-	
			-	1	-	
			-	1	-	
7.	Thasundera Singh Chowk	5	-	1	-	
			-	1	-	
			-	1	-	
			-	1	-	
			-	1	-	
8.	Mall road School	3	1	-	-	
			1	-	-	
			1	-	-	
9.	Sardar Police Station	Trillium Mall Junction	3	1	-	-
				1	-	-
				1	-	-
10.		Ratan Singh Chowk	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
11.		ESI cross Road	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
	1			-	-	
12.			6	1	-	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
		Fatehgarh Chudiyanghar Circle		1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
13.		88 Feet Road entry	4	-	1	-
				-	1	-
				-	1	-
				-	1	-
14.		88 Feet Exit	4	-	1	-
				-	1	-
				-	1	-
				-	1	-
15.		Kabir Marg	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
16.		Verka By-pass	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
					1	-
17.		Majitha By-pass	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
18.	Civil Line Police Station	Makhan Restaurant Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
19.		Crystal Chowk	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
20.		4SS Chowk	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
21.		Joshi Colony Market	5	1	-	-
				1	-	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
22.		Circular Road (opposite TSPCL office)	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
23.		Musta Chowk (Bagh chowk)	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
24.		Gala Mala Marg	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
25.		Gopal Mandir Chowk	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
26.		Hussain Pura Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
27.	Suvidha Centre	Kichlu Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
28.		District Shopping Centre	7	1	-	-
				1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	-	1
29.		C - Block market	6	1	-	-
				1	-	-
				-	1	-
				-	1	-
				-	1	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
				-	1	-
30.		Green Avenue Market	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
31.		Amrit nal Bagh	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
					1	-
32.		Gumtala Bypass	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
33.	ADCP office	Railway Station entry Point	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
34.		Railway Station exit Point	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
35.		UCO Bank (or petrol pump)	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
36.	Durgiyana Police Station	Railway Station entry / exit, B/H	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
37.		Bhandhari Bridge	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				-	-	1
38.		Hall Gate	6	-	1	-
				-	1	-
				-	1	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
				-	1	-
				-	1	-
				-	1	-
39.		Durgiyana Mandir (Hathi chowk)	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
40.		Durgiyana New Entrance	2	1	-	-
				-	1	-
Total				120	80	2

14 Appendix XI: Existing Ambient Air Quality Stations

S. No.	Name of Station
1.	Focal Point R.O. Building, Amritsar
2.	Vinod Chilling Centre, Amritsar
3.	Golden Temple, Amritsar
4.	Village Rasulpur, District Amritsar