Smart City
MISSION TRANSFORM-NATION

ASCDCL

REQUEST FOR PROPOSAL
Appointment of Master System Integrator (MSI) for supply, implementation, integration, operation and maintenance of ICT components for Aurangabad smart city

Volume II: Scope of work

Aug 2018

AURANGABAD
SMART CITY

Smart City
MISSION TRANSFORM-NATION

ASCDCL

AURANGABAD SMART CITY DEVELOPMENT CORPORATION LIMITED (ASCDCL)

APPOINTMENT OF MASTER SYSTEM INTEGRATOR (MSI)

FOR

SUPPLY, IMPLEMENTATION, INTEGRATION, OPERATION AND MAINTENANCE OF SMART CITY ICT COMPONENTS AT AURANGABAD SMART CITY

REQUEST FOR QUALIFICATION (RFQ)

CUM

REQUEST FOR PROPOSAL (RFP)

Volume II – Scope of Work

August 2018

Aurangabad Smart City Development Corporation Limited (ASCDCL)

Aurangabad Municipal Corporation, Town Hall, Aurangabad-431001, Maharashtra, India

DISCLAIMER

The information contained in this Request for Proposal document (RFP) or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by or on behalf of Aurangabad Smart City Development Corporation Limited (ASCDCL) or any of its employees or advisors, is provided to Bidder(s) on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided. This RFP is not an Agreement and is neither an offer nor invitation by ASCDCL to the prospective Bidders or any other person.

The purpose of this RFP is to provide interested parties with information that may be useful to them in making their financial offers (Bids) pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by ASCDCL in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for ASCDCL, its employees or advisors to consider the investment objectives, financial situation and particular needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in the Bidding Documents, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidder(s) is on a wide range of matters, some of which may depend upon interpretation of law. The information given is not intended to be an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law. ASCDCL accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein. ASCDCL, its employees and advisors make no representation or warranty and shall have no liability to any person, including any Applicant or Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way for participation in this Bid Stage.

ASCDCL also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. ASCDCL may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP. The issue of this RFP does not imply that ASCDCL is bound to select a Bidder or to appoint the Successful Bidder JV or Contractor, as the case may be, for the Project and ASCDCL reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

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

TABLE OF CONTENTS

DISCLAIMER i

ABBREVIATIONS ix

1. Project Overview, Brief Scope of Work and Technical Architecture Requirements 12

1.1. Technical Architecture Requirements 16
1.2. Other Requirements 20
2. Detailed Scope of Work for each Component 25

2.1 COMPONENT 1: Network Backbone 26
A. Overview 26
B. Scope of Work 27
C. Solution Requirements 28
2.2. COMPONENT 2: Command Control Centre (CCC) for Police 32
A. Overview 32
B. Scope of work 33
C. Solution Requirements 41
2.3. COMPONENT 3: City Operation Command Centre (OCC) for AMC 44
A. Overview 44
B. Scope of Work 44
C. Solution Requirement 45
2.4. COMPONENT 4: CCTV based City Surveillance System 55
A. Overview 55
B. Scope of Work 56
C. Solution requirements 62
2.5. COMPONENT 5: Biometric Attendance system 78
A. Overview 78
B. Scope of Work 78
C. Solution Requirements 81
2.6. COMPONENT 6: Smart Transport System & Smart Bus Stops 83
A. Overview 83
B. Scope of Work 84
C. Solution Requirements 92
2.7. COMPONENT 7: City Wi-Fi 95
A. Overview 95

B. Scope of Work 95
C. Solution Requirement 98
2.8. COMPONENT 8: Outdoor Digital Signage and Kiosk 100
A. Overview 100
B. Scope of Work 100
C. Solution Requirement 104
2.9. COMPONENT 9: ICT Enabled Solid Waste Management 108
A. Overview 108
B. Scope of Work 109
C. Solution Requirement 117
2.10. COMPONENT 10: Aurangabad Citizen Mobile Application and Website 122
A. Overview 122
A. Scope of Work 122
B. Solution Requirement 123
2.11. COMPONENT 11: Integration and Common Components 124
A. Overview 124
B. Scope Of work 124
C. Solution Requirement 126
3. Testing and Acceptance Procedures 128
3.1. Testing and Acceptance Procedures 128
A. Test Plan 128
B. Test scenarios 129
C. Test Execution 129
D. Testing, Commissioning & Successful Operation: 132
4. Hand holding and Training 133
4.1. Handholding and Training: 133
5. Project Implementation Timelines & Deliverables 136
5.1. Phase I – T + 1 months (T is the date of signing of the contract with MSI) 136
5.2. Phase II – T + 6 months 136
5.3. Phase III – T + 7 months 137
5.4. Phase IV – T1 + 60 months (T1 is the date of Go Live of all application) 137
6. Bill of Quantities (BOQ) 138
6.1. Command Control Center 138
6.2. Data Center 139
6.3. Operation Command Center 140

6.4. Utility Poles Passive and active components ... 141
6.5. ITMS ... 141
6.6. Smart Bus Stop ... 141
6.7. ICT enabled Waste Management Software ... 142
6.8. WIFI ... 142
6.9. Digital Outdoor Display and Kiosk ... 142
6.10. E Office ... 143
6.11. End points like cameras, ECB, PA ... 143
6.12. Licenses ... 143
6.13. SETUP at Local Police Station ... 144
6.14. Project Management & Infrastructure Set-up ... 144
6.15. Price component for OPEX ... 144
Annexure- Technical Specification Requirements ... 145
Annexure 1 – Network Backbone ... 146
Annexure 2 -Command Control Center (CCC) For Police & City Operation Command Center(OCC) for AMC ... 147
2.1 Laser Video Wall ... 148
2.2 Video Wall Controller ... 151
2.3 Integrated Building Management System (iBMS) ... 153
2.4 Monitoring Workstations/Desktop ... 156
2.5 Network Laser Colour Printer ... 158
2.6 KVM Module ... 159
2.7 Online UPS ... 160
2.8 DG Set ... 162
2.9 Structured Cabling Components &Electrical cabling component ... 164
2.10 Integrated Operation Platform (IOP) ... 165
2.11 Data Centre Specification ... 169
2.12 Core Router ... 170
2.13 Core Switch ... 171
2.14 Internet Firewall ... 172
2.15 DC Firewall ... 174
2.16 WAN Internet Router ... 177
2.17 Distribution Switch ... 178
2.18 Blade Chassis ... 179
2.19 Servers ... 181
2.20 External Storage - SAN/NAS/ Unified storage ... 182
2.21 Virtualization Software ... 184
2.22 TOR (Top of the Rack) Switch ... 187

2.23 APT (advanced persistent threat protection) ... 189
2.24 Centralized EDR ... 191
2.25 SIEM for Logs & Packets System ... 193
2.26 Application Delivery Controller ... 196
2.27 Data Leakage Prevention and Email Security ... 201
2.28 Intrusion Detection & Prevention System ... 206
2.29 SAN Switch ... 208
2.30 Storage ... 210
2.31 Smart Rack for OCC ... 212
2.32 Smart Rack for CCC ... 215
Annexure 3: CCTV based City Surveillance System ... 218
3.1 PTZ Specifications ... 219
3.2 Box Camera Specifications ... 222
3.3 Video Management System ... 225
3.4 Dome Camera Specifications ... 227
3.5 Pole for cameras ... 229
3.6 Pole for cameras (Junction box) ... 230
Annexure 4: Biometric Attendance System ... 231
4.1 Fixed Finger Scanner Specifications ... 232
4.2 Mobile Finger Scanner ... 234
4.3 Smart Rack for AMC ... 236
Annexure 5: Smart Transport system & Smart Bus Stops ... 239
5.1 Bus Stop Specifications ... 240
5.2 Roof Top Solar Panel for smart Bus Stop ... 245
5.3 Led display system for PIS ... 248
Annexure 6: City Wi-Fi ... 251
6.1 Wifi Specifications ... 252
Annexure 7: Digital display and kiosk ... 262
7.1 Outdoor Digital Display Specifications ... 263
7.2 Location and sizes of Outdoor Digital Displays ... 265
7.3 Indoor touch Kiosks ... 266
7.4 Indoor Non touch Kiosks ... 270
Annexure 8: ICT Enabled Solid Waste Management ... 273
8.1 RF ID TAG ... 274
8.2 RF ID Metal Tag ... 275
8.3 Bin Sensor ... 276
8.4 Boomer Barrier ... 276

8.5 Hand Held Bio Metrix Device 277
8.6 Weighbridge 40 MT Capacity 278
Annexure 9: Aurangabad Citizen Mobile Application and Website 280
Annexure 10– Locations 281
10.1 CCTV Camera 281
10.2 Digital Display Signages 293
10.3 Wi-Fi Hotspots 294
10.4 Smart Bus Stops - Location 296
10.6 Biometrics 297
Annexure 11: Use cases (Systems should be compatible and scalable for Phase 2 Use Cases) .. 298
Annexure 12: Indicative Design 311
12.1 Sample Design of Smart Bus Stop 312
12.2 Sample Design of Smart CCTV Pole Junction box 313
12.3 Branding Guidelines 316
12.4 Utility Pole for surveillance, smart traffic and Digital signage 317
12.5 City Network 323
12.6 Control and command centre 324
12.7 Kiosk 327
Annexure 13: Indicative length of City Network Backbone 329
Annexure 14: Information on City Bus Services 330
Annexure 15: ICT based Solid Waste Management System 330
Annexure 16: Manufacturer's Authorization (To be obtained from all OEMs) 331
Annexure 17: Equipment Details 333
Annexure 18: Deviation 334
Annexure 19: Organization Detail 335
Annexure 21: Project Implementation Methodology and Scalability 336
Annexure 22: Undertaking of Providing Training 337
Annexure 23: Undertaking Of Blacklisting 338
Annexure 24: Standards and Guidelines 339
24.1 Annex-A (Biometric Standard) 339
24.2 Annex-B (Digital Preservation Standards) 343
24.3 Annex-C (Localization and Language Technology Standard) 346

24.4 Annex-D (Metadata and Data Standards) 349
24.5 Annex-E (Mobile Governance)........ 352
24.6 Annexure-F (GIGW) 364
24.7 Annex-G (Open APIs)........ 370
24.8 Annex-H (Internet of Things) 373
24.9 Annex-I (Smart Parking) 376
24.10 Annex-J (Public WI-FI) 377
24.11 Annex-H (Disaster Management) 379
24.12 Annexure-K (BIS PIS) as per UBS-II........ 381

ABBREVIATIONS

Terms	Description
AAA	Authentication, Authorization, and Accounting
ANPR	Automated Number Plate Recognition
ASCDCL	Aurangabad Smart City Development Corporation Limited
AMC	Aurangabad Municipal Corporation
AP	Access Point
AVLS	Automated Vehicle Locator System
BOM	Bill Of Material
CCC	Command and Control Centre
CCTV	Closed Circuit Television
COP	Common Operating Platform
DBA	Database Administrator
DC	Data Centre
DCP	Deputy Commissioner of Police
DIT	Directorate of Information Technology
DNS	Domain Name Server
DR	Disaster Recovery
EMD	Earnest Money Deposit
EMS	Enterprise Management System
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
FRS	Functional Requirement Specifications
GI	Galvanized Iron
GIS	Geographical Information System
GoM	Government of Maharashtra
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global Systems for Mobile Communications
GUI	Graphical User Interface
HDPE	High-Density Polyethylene
HO	Head Office
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IOE	Internet of Everything
IP	Internet Protocol
IPS	Intrusion Prevention System
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
LED	Light Emitting Diode

Terms	Description
LOI/LOA	Letter of Intent/Letter of Award
Ltd	Limited
MoU	Memorandum of Understanding
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MUX	Multiplexer
NFC	Near Field Communication
NIC	National Informatics Centre
O&M	Operations & Maintenance
OEM	Original Equipment Manufacturer
OFC	Optical Fibre Cable
OGC	Open Geospatial Consortium
OS	Operating Systems
OTP	One Time Password
PAS	Public Address System
PDU's	Power Distribution Units
PIS	Passenger Information System
PoE	Power over Ethernet
PoP	Points of Presence
PTZ	Pan Tilt Zoom
QR Code	Quick Response Code
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RLVD	Red Light Violation Detection
RoW	Right of Way
RPO	Recovery Point Objective
RTO	Recovery Time Objective
MSI	Master System Integrator
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SMPS	Switched Mode Power Supply
SOP	Standard Operating Procedure
SOS	Save Our Souls
TRAI	Telecom Regulatory Authority of India
TRS	Technical Requirement Specifications
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VA	Video Analytics

Terms	Description
VaMS	Variable Message System
VCA	Video Content Analytics
VLAN	Virtual Local Area Network
VMS	Video Management Software/System
WAN	Wide Area Network

1. Project Overview, Brief Scope of Work and Technical Architecture Requirements

Aurangabad Smart City Development Corporation Ltd. intends to select a Master System Integrator (MSI) for the city of Aurangabad by following competitive bidding process to design, develop, implement and maintain the Smart City System for a period of five years after Go Live date on turnkey basis.

The main intent of this project is to create an integrated, innovative and inclusive architecture that allows the city to become efficient and its citizens to have a better quality of life using information that is collected from sensors and then collated, analysed and displayed or disseminated to the citizens and visitors of the city. All aspects of this tender and response will be evaluated against this objective.

MSI will develop an Integrated Smart City System that will comprise of a Command & Control Centre (CCC) for Police and City Operations Command Centre (OCC) for Aurangabad Municipal Corporation and will include the following Components in an integrated approach:

S.No.	Component	Description
1	**City Communication Network**	• MSI shall use communication (OFC) network of a Service Provider in Aurangabad for the smart city project. ▪ MSI shall make a detailed survey of communication (OFC) network of a Service Provider & electrical supply network availability of MSEDCL and GIS mapping of proposed locations of all CCTV cameras, Smart Bus Stops, IoT Sensors (Environment, etc.), Wi-Fi spots, Display Signage, Traffic Lights, Solid Waste Management Infrastructure, etc. in order to complete the various components of the Smart City project in Aurangabad.
2	**City Surveillance**	• Command and Control Centre (CCC) for Police shall be the nerve centre of City Surveillance, Traffic Management and Enforcement system. • The CCC shall be ergonomically designed with area for video wall, operators, offices, conference room, all other amenities, etc. • **MSI shall create synergies between the CCC & OCC by using an integrated architecture**

S.No.	Component	Description
		• **MSI shall setup Data Centre,** CCTV based video surveillance shall be security enabler to ensure public safety ▪ MSI shall install CCTV cameras at various location across the city for surveillance. along with Public Address System and Variable Message Signboard (VMS), Emergency Call Box/Panic Box System, etc.
3	**City Operation Command Centre (OCC) for AMC**	• City Operations Command Centre shall be the nerve centre for management and monitoring of all based ICT based Smart City components such Solid Waste Management system, smart street lighting control system, Wi-Fi, Smart Transport, Smart Bus Stops, CCTV Surveillance, Digital Signages, IoT Sensors (Environment, etc.), and PIS and all other smart city applications will be integrated, and centrally monitored, tracked and managed from the Operations Command Centre • The OCC shall be ergonomically designed with area for video wall, operators, offices, conference room, all other amenities, etc. • **MSI shall setup Data Centre, Disaster Recovery Centre & Data Backup storage facility** ▪ **MSI shall create synergies between the CCC & OCC by using an integrated architecture**
4	**Biometric Attendance System**	▪ MSI shall install Biometric (Face Recognition & Fingerprint based) attendance system for employees of AMC/ ASCDCL
5	**Smart Transport System & Smart Bus Stops**	• MSI shall install Smart Bus Stops with Digital signage, Solar PV panel, Passenger Information System (PIS), Wi-Fi spots, CCTV camera, mobile charging station, etc. including landscaping the area around the smart bus stops ▪ MSI shall integrate GPS Vehicle Tracking System, Fleet Management, Passenger Information System for Public Transport Buses/Vehicles and onboard CCTV based surveillance system
6	**City Wi-Fi Spots**	▪ MSI shall install Wi-Fi access points at identified locations in the city and at Smart Bus Stops
7	**Outdoor Digital Display & Kisoks**	MSI shall install Outdoor Digital Display & interactive and Non-interactive Kisoks in public places like railway station, airport,

S.No.	Component	Description
		mall, tourist places, bus stops etc. to display city information, tourist place video or live streaming of city event or broadcast from CCC/OCC
8	**ICT Enabled Solid Waste Management**	MSI shall install GIS/GPS enabled Solid Waste Management System to provide end to end management & monitoring of garbage collection
9	**Aurangabad Citizen Mobile Application & Website/Portal**	MSI shall develop a Mobile Application and Website/Portal integrating all the components of smart city projects to provide a platform for citizen services, complaint/ grievance management along with payment gateway integration for payment through the mobile application and website/portal.
10	**Integration Components**	MSI shall integrate the following systems with the City Operation Command Centre: • E-Governance System • Smart LED Lighting • GIS mapping for Aurangabad City Any other system

The main objective of the project is to create synergies within and across various departments of AMC for efficient city administration. To achieve this, MSI shall also ensure appropriate check points are built in the various smart city solutions. This will ensure optimum and efficient delivery of public services to the citizens and visitors of Aurangabad city.

MSI shall be responsible to carry out detailed survey prior to submission of bid for the various components of smart city solution to finalize infrastructure requirement, network bandwidth requirement, operational & administrative challenges, etc.

The subsequent sections mention the detailed scope of work, functional requirement and technical specifications for each component of smart city solution. The bidder shall note that the activities defined in the scope of work mentioned in this RFP are indicative and may not be exhaustive. MSI is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in this RFP cum RFQ and factor the same in its response.

More specifically, the following will be the activities to be carried out by MSI:

- Project Planning, Execution and Management.

- Assessment and Gap Analysis of requirement for all smart city components under scope.
- Solution Design, System Customization and development for all components mentioned in the scope of work.
- Procurement, installation, deployment and commissioning of ICT and other equipment.
- Site Preparation including required civil work associated with all components.
- LAN/WAN Networking in all components.
- Application and general awareness Training.
- Business Process Reengineering for the selected applications/ services, if required.
- STQC Certification.
- UAT & Go live.
- Training & Capacity Building & Technical Support.
- Operation & Maintenance (O & M) for 5 Years starting from Go-Live date.
- Handover Training to ASCDCL (or chosen third party) after completion of O&M period.

1.1. Technical Architecture Requirements

MSI will be required to prepare detailed Technical Architecture for various components of smart city solution as mentioned in the RFP and finalize the detailed architecture for the overall system, incorporating findings of site survey. MSI shall submit the detailed Technical Architecture and description of each component, along with the bid, ensuring compliance to the following guiding principles:

1. **Scalability:** Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of the city. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability in number of field devices, data centre equipment or other smart city components. Main technology components requiring detailed scalability planning are storage, bandwidth, computing performance (IT Infrastructure) and associated Data Centre and DR capacities.

   The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system remains operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre/ Disaster Recovery Centre infrastructure shall be capable of serving at least 1000 concurrent users.

   The Applications proposed for various solutions shall be capable of handling growth for next 5 years from Go-Live date. ***MSI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.***

2. **Availability:** The architecture components should be redundant and ensure that there are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy is to be considered at DC/DR centre components level. The system should be designed to have uptime of 99.99%.

3. **Security:** The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters, etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems, such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks shall be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavour to make use of SSL/VPN technologies to have secured communication

between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. The ASCDCL would carry out the security audit of the entire system upon handover and at regular interval during O&M period.

Field equipment installed through this Project would become an important public asset. During the contract period of the Project, the MSI shall be required to repair / replace any equipment, if stolen / damaged/faulty. Appropriate insurance cover must be provided to all the equipment supplied under this project. The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below.

a. The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols.

b. Solution shall support advanced user authentication mechanisms including digital certificates and biometric authentication.

c. Security design should provide for a well-designed identity management system, security of physical and digital assets, data and network security, backup and recovery and Disaster Recovery System.

d. Solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system.

e. The overarching requirement is the need to comply with ISO 27001 standards of security.

f. The application design and development should comply with OWASP top 10 principles.

4. **Manageability:** Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

5. **Interoperability and its Standards:** The system should have capability to take feed from cameras installed by private / Government at public places, digitize (if required) & compress (if required) this feed & store as per requirements. Keeping in view evolving needs of interoperability, the possibility that the solution shall become focal point of delivery of services and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code should not build dependency on any proprietary

software, particularly, through use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

a. At least comply with published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

b. Cyber security Model Frame work for smart city (K-15060/61/2016/SC-I)

c. Be of leading industry standards and /or as per standards

6. **Open Standards:** Systems should use open standards and protocols to the extent possible.

7. **Single-Sign On:** The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser-based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting, etc. Similarly, for external users (citizens, etc.), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check status of their applications.

8. **GIS Integration:** MSI shall undertake detail assessment for integration of all Field level ICT interventions proposed. MSI is required to carry out seamless integration to ensure ease of use of GIS in Dashboards in Command Control Centre and Operation Command Centre. If this requires field survey, it needs to be done by MSI. If such data is already available with the city, it shall facilitate to provide the same. MSI to check the availability of such data and suitability for the project. MSI is required to update GIS maps from time to time.

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

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

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

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

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

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

11. **Integration Architecture:** The integration between the various applications designed and developed for the departments concerned must follow best practice and industry standards. The Enterprise Integration Bus or similar technologies should be used to decouple the applications yet to be able to share information between them. A Common City Data Architecture and naming standards should be used across all the components. Standards should (a) at least comply with published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards.

1.2. Other Requirements

i. MSI shall engage early in active consultations with the ASCDCL, City Police and other key stakeholders to establish a clear and comprehensive project plan in line with the priorities of all project stakeholders and the project objectives.

ii. MSI shall assess existing infrastructure's current ability to support the entire solution and integrate the same with the proposed solution wherever applicable and possible.

iii. MSI shall judiciously evaluate the resources and time planned for undertaking current state assessment, given the overall timelines and milestones of the project.

iv. MSI shall be responsible for supply of all the Products/equipment such as Network, Hardware, Software, Devices, etc., as indicated (but not limited to) in the tentative Bill of Materials included in the RFP and their appropriate quantity & capacity.

v. MSI shall be responsible for supply of passive components indicated in the Bill of Materials section of the RFP viz. Housings, Fibre Patch Cords, Racks, etc.

vi. Validate / Assess the re-use of the existing infrastructure if any with ASCDCL site

vii. Supply, Installation, and Commissioning of entire solution at all the locations.

viii. MSI shall provide bandwidth required for operationalizing each smart city initiative. Bandwidth requirement shall be analysed and procured by MSI at its own cost / risk.

ix. MSI shall Install and commission connectivity across all designated locations.

x. MSI shall ensure high availability, reliability and redundancy of the network elements to meet the Service Level requirements.

xi. MSI shall be responsible for upgradation, enhancement and provisioning additional supplies of network (including active / passive components), hardware, software, etc. as requisitioned by ASCDCL.

xii. MSI shall ensure that the infrastructure provided under the project shall not have an end of life within 24 months from the date of bidding

xiii. MSI shall ensure that the end of support is not reached during concurrency of contract and 5 years thereafter.

xiv. MSI shall ensure compliance to all mandatory government regulations as amended from time to time.

xv. MSI shall ensure that all the peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, patch cords, cables, software, licenses, tools, etc. are provided according to the requirements of the solution.

xvi. ASCDCL shall not be responsible if MSI has not provisioned some components, sub-components, assemblies, sub-assemblies as part of Bill of Materials in the Bid. MSI shall have to provision these & other similar things to meet the solution requirements at no additional cost and time implications to ASCDCL.

xvii. All software licenses that MSI proposes shall be perpetual software licenses along with maintenance, upgrades and updates for the currency of the contract. The software licenses shall not be restricted based on location and ASCDCL shall have the flexibility to use the software licenses for other requirements if required.

xviii. MSI shall ensure there is a 24x7 comprehensive onsite support for duration of contract for respective components to meet SLA requirement. MSI shall ensure that all the OEMs understand the service levels required by ASCDCL. MSI is required to provide necessary MAF (Manufacturer Authorization Form) as per format provided in RFP in support of OEMs active support in the project.

xix. Considering criticality of infrastructure, MSI is expected to design the solution considering RFP requirement of no single point of failure with high level of redundancy and resilience to meet the network uptime requirements.

xx. MSI shall be responsible for periodic updates & upgrades of all equipment, cabling and connectivity provided at all locations during the contract period.

xxi. MSI shall be responsible for setting up / building / renovating the necessary physical infrastructure including provisioning for network, power, rack, etc. at all the locations.

xxii. MSI is expected to provide following services, including but not limited to:

- Provisioning hardware and network components of the solution, in line with the proposed ASCDCL's requirements
- Size of network devices (like router, switches, security equipment including firewalls, IPS/IDS, routers, etc. as per location requirements with required components/modules, considering redundancy and load balancing in line with RFP.
- Size and provision the LAN/WAN bandwidth requirements across all locations considering application performance, data transfer, CCC/OCC, DC/DR and other requirements for smart city initiatives.
- Size and provision the internet connectivity for Service Provider network and Network Backbone.
- Liaise with service providers for commissioning and maintenance of the links.
- Furnish a schedule of delivery of all IT/Non-IT Infrastructure items
- All equipment proposed as part of this RFP shall be rack mountable.
- ASCDCL may at its sole discretion evaluate the hardware sizing document proposed by the MSI. MSI needs to provide necessary explanation for sizing

- Complete hardware sizing for the complete scope with provision for upgrade
- Specifying the number and configuration of the racks (size, power, etc.) that shall be required at all the locations.
- MSI shall provide for all required features like support for multiple routing protocols, congestion management mechanisms and Quality of Service support.
- MSI shall ensure that all active equipment (components) are Simple Network Management Protocol (SNMP) V3 compliant and are available for maintenance/ management through SNMP from the date of installation by a Network Monitoring System.

xxiii. MSI shall directly interact with electricity boards for provision of mains power supply at all desired locations for any Field Infrastructure solution. ASCDCL shall facilitate, if any documentation is required from its side. MSI shall be responsible for provisioning of requisite electricity power and its recurring charges (during operational phase). MSI may provision the same under appropriate heads in the commercial bid.

xxiv. All existing road signs which are likely to be affected by works are to be carefully taken down and stored. Signs to be re-erected shall be cleaned, provided with new fixings where necessary and the posts re-painted in accordance with ASCDCL guidelines. Road signs, street name plate, etc., damaged by MSI during their operation shall be repaired or replaced at MSI's cost.

xxv. The existing field Infrastructure including the poles, cantilevers, aspects, controllers and cabling and associated mountings and civil infrastructure may need to be dismantled (where ever applicable) and replaced with the new systems proposed and shall be in the scope of MSI. The dismantled infrastructure shall be delivered at ASCDCL designated location without damage, at no extra cost.

xxvi. Prior to starting the site clearance, MSI shall carry out survey of field locations, for buildings, structures, fences, trees, existing installations, etc. ASCDCL shall be fully informed of results of survey and amount and extent of demolition and site clearance shall then be agreed with AMC.

xxvii. Lightning Proof Measures

- MSI shall comply with lightning-protection and anti-interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying.
- Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof functions; capable to bear certain mechanical external force.
- Signal separation of low and high frequency; equipment protective field shall be

connected with their own public equal power bodies; small size/equipment signal lightning arrester shall be erected before the earthling.

- Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security system, server data path and other communication equipment.
- Data line protection shall be installed as per zone defined in IEC 62305.

  i. Type 1 device shall be installed between zone 0B and zone 1

  ii. Type 2 devices shall be installed before the equipment in zone 2 and 3

xxviii. After signing of contract, MSI needs to deploy team proposed for the project and ensure that a Project Inception Report is submitted to ASCDCL, covering following aspects:

- Names of Project Team members, their roles & responsibilities
- Approach & methodology to be adopted to implement the Project (which should be in line with what has been proposed during bidding stage, but may have value additions / learning in the interest of the project).
- Responsibility matrix for all stakeholders
- Risks the MSI anticipates and plans they have towards their mitigation.
- Detailed Project Plan, specifying dependencies between various project activities/ sub-activities and their timelines.

xxix. Feasibility Report for all ICT projects should be conducted. As part of feasibility report, MSI should provide detailed To-Be designs (Junction layout plans) specifying following:

- High Level Design (including but not limited to)
  - i. Application architecture documents
  - ii. ER diagrams and other data modelling documents
  - iii. Logical and physical database design
- Data dictionary and data definitions
  - ▪ Application component design including component deployment views, control flows, etc.
  - ▪ Field equipment deployment architecture
  - ▪ Low Level Design (including but not limited to)
    - o Application flows and logic including pseudo code
    - o GUI design (screen design, navigation, etc.)

  - o Database architecture, including defining data structure, data dictionary as per standards laid-down by GoI/ Government of Maharashtra

- Location of all field systems and components proposed at junctions/other locations,
- Height and foundation of Traffic Signals and Standard Poles for Pedestrian signals.
- Height and foundation of poles, cantilevers, gantry and other mounting structures for other field devices
- Location of Junction Box and PoP
- Electrical power provisioning

xxx. For all the ICT components and facilities covered under the scope that are publically visible, MSI shall have provision to enable ASCDCL and Smart City branding identification. MSI shall get the design of applying the established branding identification, colouring, etc., approved by ASCDCL prior to implementing the same.

xxxi. MSI shall provide Standard Operating Procedures (SOPs), and User Manuals including a step-by-step instruction to operate and to resolve the situation quickly and easily.

xxxii. Any functionality not expressly stated in this document but required to meet the needs of the project to ensure successful operations of the system shall essentially be under the scope of MSI and for that no extra charges shall be admissible.

xxxiii. Technical specifications mentioned in the Annexures shall be applicable. Additionally, applicable government standards and guidelines shall be complied with. Technical solutions offered by MSI must also comply with Use Cases as per Annexures and should include provision for future addition to Use Cases.

2. Detailed Scope of Work for each Component

MSI will be implementing the solution as per requirement and design principle mentioned above.

There are several components to be implemented and integrated in the city which will converge in to command and control centre, MSI must use existing infrastructure as much as available in city below are the details of components to be implemented by MSI during this project:

MSI must implement all use cases as per Annexures.

2.1 COMPONENT 1: Network Backbone

A. Overview

City Communication Network: MSI shall use communication (OFC) network of a Service Provider in Aurangabad for the smart city project.

MSI shall make a detailed survey of communication (OFC) network of a Service Provider & electrical supply network availability of MSEDCL and GIS mapping of proposed locations of all CCTV cameras, Smart Bus Stops, IoT Sensors (Environment, etc.), Wi-Fi spots, Display Signage, Traffic Lights, Solid Waste Management Infrastructure, etc., in order complete the various components of the Smart City project in Aurangabad. With technology being a key driver for implementation of smart city initiatives across Aurangabad, a robust network is one of the key foundational requirements on which future ICT based 'Smart' initiatives shall be designed and built. Accordingly, Authority has decided to use service provider for a city-wide network backbone infrastructure that shall act as the backbone for effective implementation of smart city initiatives across Aurangabad.

The service providers network backbone infrastructure shall be capable to carry all the key services that shall be implemented in due course under smart city initiatives. Service provider should have largest underground fibre network and should have readiness to give needed connectivity at very short notice.

The expected benefits to be derived from city network backbone are:

1. Connectivity – Network that interconnects citizens, government, business and communities.
2. Smartness – Network that allows better management and control to offer richer application experiences.
3. Secure, private and resilient – Network built considering security standards and best practices with stability in bandwidth provisioning and resilience.
4. Efficient – Network that is capable to deliver the envisaged bandwidth and related services.
5. Scalable – A network that can scale up to cater all the required bandwidth for deployment of future smart city initiatives.

MPLS based network or better is expected to be provisioned for the backbone network.

The network backbone is expected to help Aurangabad build a converged network, bringing together different city management vertical solutions on a single foundational network infrastructure. The converged network shall facilitate information exchange between resources and applications across different domains. It is proposed to be an end-to-end platform enabling delivery of varied services for citizens. Key objectives envisaged are to provide:

1. IP connectivity that shall enable the citizens to avail varied services under smart city initiatives
2. Wired and wireless, scalable, and highly secure network platform
3. Data management framework to help enable data collection, organization, and sharing
4. Adoption and usage of distributed compute and storage services, location services, and security services

B. Scope of Work

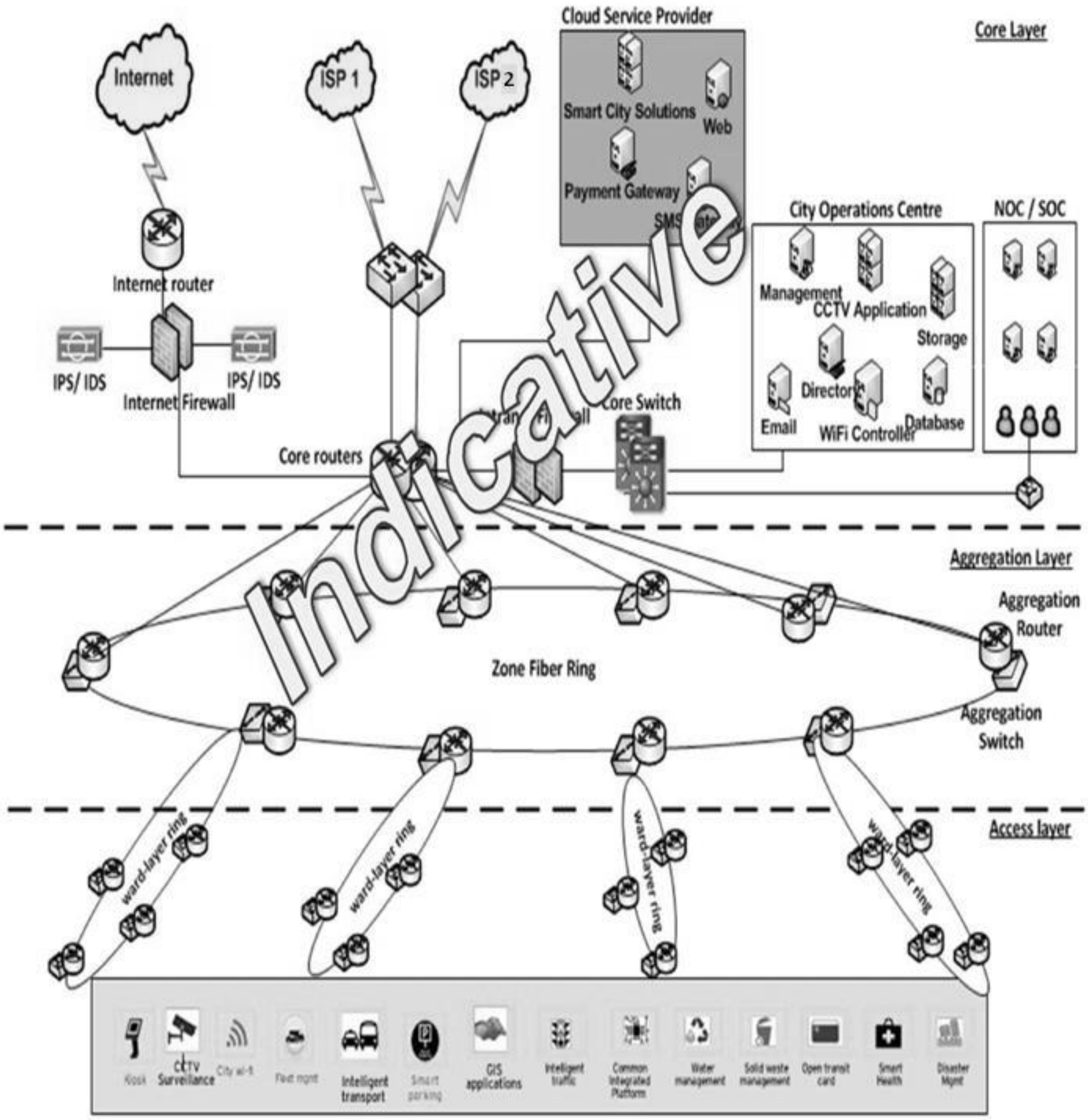
1. MSI should tie up with an Internet Service Provider or Telecom Service Provider to provide connectivity from Field Device Infrastructure to CCC/OCC/Data Centre/ Disaster Recovery Centre / and ASCDCL Offices as required.
2. MSI should tie up with an ISP who has Largest/widest network available in term of connectivity to the field location mapped and ready to do Provision at very short notice maximum of 8 weeks to the area where connectivity not available currently.
3. MSI should use secure public internet for transmission of information between field devices infrastructure to the core router of CCC/OCC. Required security applications should be factored in to avoid security breaches at field devices infrastructure level.
4. MSI should estimate the bandwidth requirement for connectivity between CCC/OCC/ Data Centre/ Disaster Recovery Centre and the same shall be clearly provisioned in the technical proposal with detailed calculations.
5. Connectivity between CCC/OCC/Data Centre/ Disaster Recovery Centre shall be through Local/Wide Area Network (LAN/WAN).
6. Bandwidth provisioned needs to adhere to performance benchmark of IOT end points of latency jitter and packet loss
7. MSI shall meet the parameters of video feed quality, security & performance. MSI should factor the same while designing the solution.
8. Performance and event of entire network must be connected to Network operating center NOC with over all operational and performance reporting real time
9. 24*7 operational support from NOC must be provided by service provider.

C. Solution Requirements

- **Functional design**

  The overall functional design of network backbone is indicative in nature and is envisaged to be implemented in a three-tiered architecture. However, the standards of design and services should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned at Annexure –XI.

The 3-tier architecture as below is indicative and the SI is required to propose its own architecture in the technical bid.



The envisaged layers of the City Network Backbone are:

a. **Core Layer:** The Core layer forms the backbone of the entire network which consists of Compute, storage, application, links and connectivity to be established at the command control center and City Operations Centre. This layer shall enable all applications hosted at command control center and City Operations Centre to be accessed over the backbone for consumers and users. Core layer shall form the point of aggregation for all the traffic coming from the Zone layer and beyond.

b. **Aggregation Layer – Zone Level:** The aggregation layer is envisaged at Zone level. The traffic coming from respective wards shall get aggregated at the Zone level. Ring architecture is proposed to be formed to establish the required redundancy. The aggregation layer shall further connect to the Core layer for forwarding the traffic to the Core layer.

c. **Access Layer –Ward Level**: The Access layer shall be formed at the wards of authority. All the wards in the respective zone shall form individual rings to establish redundancy.

   There can be multiple rings within the respective zone. For example, if there are 10 wards in a given zone, then two rings comprising of 5 wards each can be created. These two rings shall ultimately connect to the respective zone (PoP). The access layer shall enable the smart city solutions to connect to the network backbone. The aggregation switch of the respective smart city solution shall tap on the respective access layer devices.

d. **Services Layer – Smart City Solution Level**: The Service layer shall be formed at various locations within the city. The service layer shall enable the smart city solutions such as City Surveillance, City WiFi, Smart lighting, Smart parking, smart traffic, etc., to connect to the network backbone. The aggregation switch of the respective smart city solution shall connect on the Access layer devices to connect to the network backbone

Various locations for deployment of above layers:

Sr. No	Item	Location of Deployment
1	Core layer	Command control center and city operation center.
2	Aggregation layer	Identified aggregation point as mentioned in ANNEXURE V. These are mostly Authority zonal offices and tentatively identified government office buildings. A Minimum of 10 such aggregation points are being considered. SI may estimate and propose the number of aggregation points.
3	Access layer	Aggregation points to be identified by SI based on network load and geographical coverage. A Minimum of 10 rings for access layers to be considered by SI. These may overlap in order to provide required redundancy.
4	Services layer	• The services layer is considered to be the edge locations/area where the smart city solutions such as the following shall be deployed: City Surveillance • City WiFi • ICT based Solid waste, management • Smart Lighting • Smart traffic • Smart Parking • City Bus Intelligent transport system, • Environment sensors • E-governance

- **Key services which shall be provisioned under various layers:**

1. Monitoring and Management – The management and monitoring layer shall be provisioned centrally from core layer. Centralized management of infrastructure resources shall be implemented in core, aggregation layer, zonal layer and ward layer. All key services that shall be provisioned for the users such as –

    a. City Wi-Fi

    b. CCTV surveillance

    c. All other Smart City initiatives

2. Network Operation Centre (NOC): The NOC shall consist of two layers:

    a. Core layer: This shall monitor all the infrastructure devices (Router, switches, firewall, bandwidth, etc.) that are kept in core layer, aggregation layer along with key services that shall be provisioned in due course.

    b. Aggregation layer: The aggregation layer shall help in monitoring the issues related to fibre, network, infrastructure implemented at zone layer and ward layer.

3. Configuration and change management: Configuration shall be managed from core layer for all the devices 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 the Authority.

4. The proposed solution shall be scalable in nature to host all key services under smart city

5. The proposed solution shall have redundancy built at each layer

6. The proposed solution shall be capable to allow enough redundancy built at fibre as well as at infrastructure level

7. The proposed solution shall be ready to scale up both horizontally and vertically

8. The proposed solution shall be ready in all respect where it is envisaged by Authority to make use of this infrastructure under different revenue models under its long-term vision.

9. The solution shall meet demands of bandwidth needs for all the procured and planned smart city solutions

10. The solution shall easily integrate with WiFi subsystem that shall be connected on the same backbone infrastructure.

11. The solution shall be ready in all aspects to host FTTX model in near future to provide voice, video and data services over fibre.

2.2. COMPONENT 2: Command Control Centre (CCC) for Police

A. Overview

State-of-the-art Command Control Centre is required to be established as part of the City Surveillance solution. The proposed CCC shall handle feeds from field cameras and display them on the video wall in the CCC and provide necessary interface for integrating with other applications like Dial 100 and response mechanism as required by ASCDCL, it shall present a Common Operating Picture (COP) of real time events in the area of surveillance. Functions of the Command Control Centre shall include but not limited to the following:

- Video Surveillance
- Video Investigations
- Emergency Response activities
- Data Centre (data storage & retrieval)

Command Control Centre shall work in fully automated environment for optimized monitoring, regulation and enforcement of traffic with various law enforcement services. Various applications/ modules like ANPR/RLVD/E-Challan specified in this RFP shall be integrated into one functional system and shall be accessible by operators and concerned agencies with necessary login credentials. The operators shall be able to access master data like Vahan and Sarathi databases (that are available with the government agencies which can be integrated). The integration with such systems will be in the scope of MSI.

Location for Command Control Centre shall be provided by ASCDCL. Responsibilities of MSI shall include site preparation activities. MSI shall ensure that the Command Control Centre shall manage, control and integrate various systems in a seamless manner.

Command Control Centre shall provide a comprehensive system for planning, optimizing resources and response. The system shall thus be an “end to end” solution for safeguarding and securing people and assets.

MSI shall be required to undertake detailed assessment of requirements at Command Control Centre and prepare a plan to implement Command Control Centre and commission required IT and non-IT infrastructure and civil/structural/ electrical work as required.

Data and surveillance network shall share the same physical infrastructure with guaranteed bandwidth for each individual segment. The software components should provide comfortable monitoring experience, easy extraction of clips and management of storage.

The video feed from surveillance cameras shall be received at Command Control Centre where a video wall shall be installed for viewing. The surveillance team shall receive live feeds from surveillance camera and shall also control PTZ camera using joysticks. They shall be alerted if an incident is detected through video content analytics events generated from various sensors sending feed to Command Control Centre and shall be able to view relevant feed from surveillance cameras. The operator on each workstation shall be able to work on multiple monitors at the same time, for which there multi screens with one computer (specifically three) to be installed on work desks (with appropriate ergonomical furniture) with appropriate multi monitor mounts.

The Command Control Centre will be the nerve centre for monitoring and management of all surveillance cameras for crime management and traffic enforcement. The centre will have a video wall which will display the video feed from various field CCTV cameras. The CCC will be manned by at least 20 operators and will be equipped with all office infrastructure such as cubicle, cabins, conference, meeting room, etc.

A common Data Centre and Disaster Recovery Centre for the CCC and OCC will house the entire IT and related infrastructure.

B. Scope of work

Data center

Design, Supply and Deployment of IT Infrastructure for DC:

a) **Hardware and Network Provisioning:**

MSI shall be responsible for following but not limited to:

- Appropriate sizing and provisioning of IT infrastructure like servers/storage, network devices (like routers/switches, etc.), security equipment including firewalls, etc. with the required components/modules considering redundancy and load balancing in line with minimum technical requirements
- Warranty for all IT hardware assets procured to comply with the requirements as defined in this RFP.
- Size the bandwidth requirements across all locations considering the application performance, replication, data transfer, internet connectivity for DC and other requirements.
- Furnish a schedule of delivery of all IT Infrastructure items
- Ensure all hardware requirements of application suite (including third party applications), databases, OS and other software are met.
- ASCDCL may at its sole discretion evaluate the hardware sizing. The MSI needs to provide necessary explanation for sizing to ASCDCL
- Ensure that the servers should accommodate newer versions of processors, memory, etc. that support enhanced capability (e.g. lower power footprint,

higher working temperature, smaller process architecture, higher frequency, etc.) of operation if required, whenever they are available. To further clarify, motherboard, controllers, etc. provided shall be of latest architecture available that supports such newer version. MSI shall substantiate with proof; preferably with an undertaking to replace the processors as and when such processors of highest level of frequency are supported.

- Server models wherever applicable shall be Blade Mount servers with key board, monitor, etc. shared to minimize the requirement of rack space in DC & DR considering any space constraints.

b) Provisioning Switches:

- MSI shall size and propose requisite switches at DC & DR with the required components/modules considering redundancy and load balancing.
- MSI shall size and propose other switches required for interconnecting various segments, operations centre, work area, etc.

c) IP Address Schema:

- MSI shall design suitable IP Schema for entire Local Area Network including DC & DR and interfaces to external systems/network. MSI shall ensure efficient traffic routing irrespective of link medium.
- MSI shall maintain the IP Schema with required modifications from time to time during the project period.
- MSI should provide unique identity schema similar to addressing schema for all hardware components.

d) Sub-Networks & Management of Network operation

- Architecture of DC & DR shall be divided into different sub-networks. These networks shall be separated from other networks through switches and firewalls. Logical separations of these sub-networks shall be done using VLAN.
- Separate VLAN shall be created to manage the entire network. This network shall have systems to monitor, manage routers, switches, Firewalls, etc. The MSI shall provide necessary hardware / server for loading the monitoring software if required.

e) Provisioning Storage

- Storage requirements for the application suite shall have to be assessed by MSI and the storage solution shall be sized and procured accordingly. MSI shall propose appropriate storage mechanism to accommodate proposed application suite requirement of ASCDCL.
- Proposed storage shall be configured with appropriate redundancy to maintain business continuity.

f) Network Equipment level redundancy

- MSI shall provide real-time redundancy at the network equipment level in Data Centre, and there shall not be any single point of failure.
- All equipment shall be provided with dual power supply modules. Each of the two supply modules shall be connected to alternate power strips of the network rack (two power strips to be provided in each network rack).
- Network Equipment redundancy stipulations wherever prescribed are minimum requirements that MSI needs to consider. However, MSI needs to estimate and plan actual requirements considering service level requirements specified in this RFP.

g) Provisioning IT Security Equipment

- MSI shall size & propose firewalls with required components/modules for DC/DR.
- Necessary IDS/ IPS shall be provided for monitoring traffic of all VLANs at DC/DR.
- Necessary devices for log capture from servers, network equipment and other devices shall to be provisioned.
- MSI shall implement DNS server so that the URL can be used instead of accessing web server using IP address directly. The required Hardware and Software for DNS server at DC & DR shall be provisioned by MSI.
- MSI shall implement management systems and procedures that adhere to ASCDCL's security policies.
- MSI shall secure network resources against unauthorized access from internal or external sources.
- MSI shall also provide a mechanism for tracking security incidents and identifying patterns, if any. The tracking mechanism shall, at a minimum, track the number of security incident occurrences resulting in a user losing data, loss of data integrity, denial of service, loss of confidentiality or any incident that renders the user unproductive for a period of time
- MSI shall ensure that all firewall devices are staged and comprehensively tested prior to deployment. In addition, SI shall conduct a vulnerability scan and analysis of the network to ensure that the optimal policies are instituted on the firewall.
- MSI shall ensure that all firewall management is initiated from a segregated management rail on the network.
- MSI shall provide intrusion management services to protect ASCDCL's resources from internal and external threats.
- MSI shall provide ASCDCL with the necessary hardware/software required for efficient intrusion management.

Both DC and DR site shall have built in redundancy and high availability in compute and storage to ensure that there is no single point of failure. There shall be no loss of video recording in a CCC in case of failure of any single server and storage component.

Both DC and DR Site shall work in an Active-Active mode.

MSI shall establish dedicated connectivity between DC & DR Site for replication & failover. MSI shall design the DC and DR solution with the necessary load balancing, replication and recovery solution that provide zero RPO (Recovery Point Objective) and RTO (Recovery Time Objective) of 10 minutes.

DC and DR site shall be periodically audited, updated and mock drills shall be performed along with the findings and improvement /corrective steps to be taken to concerned ASCDCL.

MSI shall submit the detailed solution document for DC and DR Site solution with justification for the proposed design meeting the requirements along with the bid.

h) Back Up Software:

- Backup solution shall have same GUI across heterogeneous platform to ensure easy administration and available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup/ restores from various supported platforms.
- Backup Solution should have ability to backup data from one server platform and restore it to another server platform to eliminate dependence on a particular machine and for disaster recovery purposes.
- Backup Solution should support various level of backups including full, incremental, and user driven backup along with various retention period.
- Backup clients should be updated automatically using the client push feature
- Backup should support agentless backup for virtualization platform with non-staged granular recovery.
- Backup Software should support intelligent policy for virtualization.
- Backup Software must provide Source (Client & Media Server) & Target base data deduplication capabilities.
- Backup Solution should Integrate with third party VTL, NAS, SAN which has data deduplication capabilities and Robotic/automated Tape library
- Backup Solution must have Wizard-driven configuration and modifications for backup, restoration and devices.
- Backup solution shall have in-built frequency and calendar based scheduling system.
- Backup Solution must have Optimized way for data movement from client to disk target.
- Backup Solution should support (inflight & at rest) encryption.
- Backup solution shall support tape mirroring of the same job running concurrently with primary backup.
- Backup solution shall allow creating tape clone facility after the backup process.

- Backup Solution should have Capability to do trend analysis for capacity planning of backup environment.
- Backup Solution must offer capacity-based licensing. License should be for the front-end capacity rather than back-end. There should be no incremental cost associated with longer retention periods.
- Backup solution should not require purchase of additional licenses for DR sites (copies of original data), also should not require purchase of additional licenses for replication to DR sites.
- Software license should be independent of hardware so replacing hardware should not incur new software license cost.
- Backup solution must include Agent/Modules for online backup of files, applications and databases such as MS SQL, Oracle, DB2, Sybase, Exchange, SharePoint and File share backup(SMB)
- Backup solution should provide recovery from physical servers to Virtual and image level recovery.
- Backup solution should have DC/DR plug-ins for backup data replication.
- Backup Solution should have Inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.
- Backup Replication at DR site, DC/DR. Replication license should be included as part of solutions.
- Backup software should support multiplexing and multi streaming and shall support the capability to write up to Min 32 data streams.
- Backup Solutions should have capabilities to tape/disk out backup catalogue and deduplication catalogue.

Backup solution should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data. De-duplication engine should also facilitate IP base replication of de-dupe data; without any extra charge.

Enterprise Management System (EMS)

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

- Network Monitoring System
- Server Monitoring System
- Helpdesk System

The solution should provide a unified web based console which allows role based access to the users.

Network Monitoring System

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

- Proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- System must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.

System should be able to clearly identify configuration changes and administrators should receive an alert in such cases

Server Monitoring System

- Tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
- Tool must provide information about availability and performance for target server nodes.

Tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable

Helpdesk System

- Proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.
- Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
- Helpdesk should be an ITIL certified tool for Incident, Problem, Change, Knowledge, Configuration and SLA Management processes.

- Helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
- Solution should provide a clustered view of recurring themes hidden in the huge quantities of data for spotting service desk trends easily
- Helpdesk should have capability to automatically categorize, understand the impact, and assign the service desk ticket to relevant helpdesk team members
- Centralized Help Desk System should have integration with Network / Server Monitoring Systems so that the Help Desk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what alarms corresponding helpdesk tickets got logged.
- Helpdesk should have an integrated CMDB to automatically collect and manage accurate and current business service definitions, associated infrastructure relationships and detailed information on the assets
- It must be a centralized monitoring solution for all IT assets (including servers, field level infrastructure etc.)
- Solution should provide inventory of all the discovered devices. Out of box inventory fields should be available and it should have provision to add additional fields as required
- SLA & Contract Management module of helpdesk should be able to capture all the System based SLAs defined in this RFP and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources. SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs.
- Helpdesk must have integrated dashboard providing view of non-performing components / issues with related to service on any active components
- Solution must support Service Level Agreements version control and audit Trail to ensure accountability for the project.
- Solution should support requirements of the auditors requiring technical audit of the whole system.
- Solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- Solution should support SLA Alerts escalation and approval process.

A general process flow for the helpdesk management is depicted in the flow chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with ASCDCL prior to Go Live date.

Reporting

- Solution should provide historical and concurrent service level reports to ensure accountability of the service provider's performance
- Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Excel, Adobe PDF etc.
- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, Capacity planning reports etc.)
- Solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- Resource utilization exceeding or below customer-defined limits
- Resource utilization exceeding or below predefined threshold limits
- Network Management function should be able to do traffic analysis. Traffic Analysis must include Bandwidth Utilization patterns by protocol/source/destination, Network Response time patterns for various applications over the network. It should help with out of the box analysis reports to understand top bandwidth consumers by application, source, or destination. It should help with advanced reporting features to provide various reports that help understand capacity needs of the network bandwidth based on current utilization and response time trends.
- Discovery must also support device redundancy discovery in case of virtual IP addresses using vendor specific protocols such as VRRP and HSRP.
- Solution should be able to also provide a threshold and profile capability on the KPIs monitored on the network to understand the impact of failures and degradations which eventually results in revenue loss.
- Should support automatic base lining on historical data, and thresholds that can be adjusted as required, based on data collected
- Solution should offer off-the-shelf Reports for KPIs such as Availability, Uptime, and Resource

Centralised Antivirus Solution

The following features are required for centralized anti-virus solution, to protect all computing resources (servers, desktops, other edge level devices, etc.) across the entire MSI provided hardware and also existing ASCDCL infrastructure:

- Ability to scan through all file types and various compression formats. Ability to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls.
- Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- Shall provide Real-time Product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- The solution must provide protection to multiple remote clients

- Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- Should be capable of providing multiple layers of defence
- Shall have facility to clean, delete and quarantine the virus affected files.
- Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.
- Should support in-memory scanning so as to minimize Disk IO.
- Should support Multi-threaded scanning
- Should support scanning of nested compressed files
- Should support heuristic scanning to allow rule-based detection of unknown viruses

All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security.

C. Solution Requirements

Data Centre

The Data Centre and it corresponding HA/DR site will be the nerve centre wherein all the ICT infrastructure along with the network infrastructure will be installed. The data centre will host all the software applications for various smart city components. The data centre will have adequate provision for data security through implementation of firewall, IPDS, antivirus system, etc. The Physical access to the data centre will also be managed through a biometric access system.

The Disaster Recovery Centre will serve as a platform for making all the applications hosted at the data centre available in the event of a failure or a disaster. In case of non-availability of data centre, the DR centre should be able to operate all the applications for the smart city components. The DR centre will have all the functionality and infrastructure similar to the data centre. It will be possible to run the OCC and CCC interchangeably in case there is an outage in any of the centres due to any issue.

The physical location of the Data Centre and the DR site will be determined based on the projections of the MSI and will be provided by ASCDCL. All civil, mechanical and electrical work associated with creating the facility will be in the scope of the MSI.

Appropriate network infrastructure between the DR Site & DC connected to the two command centres will be created to make this a seamless system.

- MSI is required to locate all hardware/software and related items as per design offered for smart city infrastructure including SLA monitoring and Help desk management, in above data Centre complying with standard guidelines as per Telecommunications Infrastructure UPTIME/TIA-942.

- Data Centre shall be available for 24 x 365 operation.
- Smart city infrastructure shall have built in redundancy and high availability in computing and storage to ensure that there is no single point of failure.
- MSI shall locate the Data Centre in the space provided by AMC/ASCDCL in Aurangabad city, since this is one of the most critical components of smart city infrastructure. System SLA as defined in the RFP to be met solely by MSI.
- MSI shall submit to ASCDCL adequate documentation/ evidences in support of the choice of the data Centre to meet the project requirements.
- Minimum Guiding factors for selection of Data Centre: Following are benchmark requirements which should act as guiding factors for MSI to select and propose locations for Data Centre
  - There should be dedicated rack space available in the Data Centre for entire smart city solutions / infrastructure.
  - Access to Data Centre Space where the Smart City Project Infrastructure is proposed to be hosted should be demarcated and physical access to the place would be given only to the authorized personnel
  - Smart Racks system with Redundant precision air conditioners, power sources, fire suppression system along with access control system at rack level
  - Smart City Data Centre should be as per Telecommunications Infrastructure Standard for Data Centres and should be 27001 Certified. The required certification to be enclosed along with the technical bid response.
  - It should have access control system implemented for secured access.
  - Indoor CCTV Cameras would be required to be installed to monitor the physical access of the system from remote location
  - Physical Access to the building hosting Data Centre should be armed and it must be possible to even depute police personnel for physical security of the premises.
- Minimum 30 days data backup of video feeds and transaction data for minimum 1 year shall be stored within the Data Centre infrastructure.
- In case the Data Centre services are to go down due to any unforeseen circumstance, the Command Centre should have access to video feeds of previous 90 days and transaction data for min 1 year from this data backup facility.
- Access logs to be stored for entire duration of contract and handed over to ASCDCL upon termination/expiry of the contract.

DC Minimum characteristic:

- Data Centre Availability: The availability of data from the hardware at a location must be guaranteed to 99.982% availability.
- Redundancy and concurrent maintainability. It requires at least n+1 redundancy as well as concurrent maintainability for all power and cooling components and distribution systems. Any such component’s lack of availability due to failure (or maintenance) should not affect the infrastructure’s normal functioning.

- No more than 1.6 hours of downtime per year
- N+1 fault tolerant providing at least 72 hour power outage protection
- All IT equipment should be dual-powered and fully compatible within the topology of site architecture.

Data Centre shall primarily be divided into two zones:

- Server Infrastructure Zone: This zone shall host servers, server racks, storage racks and networking components like routers, switches to passive components. All the Data Centre LAN connections shall be provided through switches placed in this area. Access to this zone, where the surveillance project IT infrastructure is hosted, shall be demarcated and physical access to the place shall be given only to authorized personnel. Indoor CCTV Cameras shall be installed to monitor physical access of the system from remote location.

- UPS and Electrical Zone: This zone shall house all the Un-Interrupted Power Supply units, Main Power Distribution Units (PDUs) to feed the components such as PAC, UPS, lighting, fixtures etc. This shall also house all the batteries accompanying the UPS components. As these generate good amount of radiation, it is advised to house these components in a room separate from server infrastructure zone.

DR Disaster Recovery Site

- MSI is required to provision for a Disaster Recovery (DR) Centre same as of main Data Centre (DC) capacity & standard for Smart City Solution.
- MSI should provision cloud base the Disaster Recovery (DR) Centre
- DR site shall provision to cater to 100% load of smart city system.
- There shall be no loss of video recording in case of failure of any single server and storage component. Both DC and DR Site shall work in an Active-Active mode with 100% recording of cameras and application availability of all smart city components.

MSI shall establish dedicated connectivity between the DC and DR Site for replication & failover. MSI shall submit the detailed solution document for the DR Site with justification for proposed design meeting the requirements.

MSI shall provide Standard Operating Procedures (SOPs), and user Manuals a step-by-step instruction to operate and to resolve the situation quickly and easily. Smartcity ASCDCL branding at appropriated and aesthetic location in CCC.

Technical specifications mentioned in the Annexures shall be applicable. Additionally, applicable government standards and guidelines shall be complied with.

Technical solutions offered by MSI must also comply with Use Cases as per Annexures and should include provision for future addition to Use Cases.

2.3. COMPONENT 3: City Operation Command Centre (OCC) for AMC

A. Overview

The main objective of a City Operation Command Centre (OCC) is to break silos between departments and within departments, and integrate processesto serve public in an efficient manner. As part of Aurangabad Smart City, it is proposed to build one common operation centre. This centre will provide an integrated view of all smart component projects identified in this document, its primary focus is to serve as a decision support engine for city administrators in day-to-day operations or during emergency situations.

This centre, shall leverage information provided by various departments and provide a comprehensive response mechanism to the day-to-day challenges across the city. City Operation Centre shall be fully integrated solution that provides seamless incident – response management, collaboration and geo-spatial display. Various ICT projects shall be able to use the data and intelligence gathered from operations of other elements so that civic services are delivered more efficiently and in an informed fashion.

MSI shall develop application module for the smooth operation of City Operation Command Centre, and shall deploy support and maintenance manpower at the OCC. To ensure that ICT systems are delivered at the performance level envisaged, it is important that an effective monitoring and management system be put in place. It is thus proposed to have a proven Enterprise Management System (EMS) for the efficient management of the system, reporting, SLA monitoring and resolution of issues.

B. Scope of Work

a) MSI should inspect the location and factor in amount of work needed to build OCC in the bid document. MSI should provide a universal dashboard to view all applications in a consolidated manner on GIS map provided by ASCDCL and also general KPI View.

b) MSI should be able to provide Unified view for each Departments on GIS map provided by ASCDCL and general KPI views.

c) MSI should also continuously monitor Field infrastructure/Servers/Routers/CCC which has been built as part of this RFP

d) KPI’s which need to be tracked & projected on video wall shall be agreed during inception stage

e) Key KPI for each domain needs to be tracked:

- KPI’s list given are indicative and a detailed list of KPI’s need to be furnished by MSI during feasibility study
- KPI’s should include from the following categories
    - Process KPI: KPI’s which measure the efficiency of integrated processes

- Event Based KPI

f) System should create new KPI's on the fly.

g) MSI should setup a dedicated helpdesk to support field infrastructure laid.

C. Solution Requirement

- Space should be provided for teams from different departments

City Operations Platform - Functional Specifications:

a) Integrated Operations Platform (IOP) shall have IoT Platform Software (Data Normalization software) & City Operation Centre Software functionalities;

b) All applications which have field infrastructure like – Smart Transport, Smart Traffic, Solid Waste Management, etc., proposed to be built as part of Smart City initiative shall pass information processing via IoT Platform.

c) IoT Layer must integrate lots of Services in the current scenario and must deliver an architecture which will be future scalable and can accommodate more Services / Utility Solution Integration.

d) IoT shall be a Common layer and is required for the Normalization of the data from different edge applications. This layer will aggregate and integrate utilities & sensors data to ensure that Device management, Analytics, Reporting, Dash-boards and integration of the Different authorities/department data can be performed from a single operational screen. This layer shall also integrate with different Independent Software Vendor (ISV) applications hosted at Data Centre.

Integrated Operation Platform (IOP)

With the increasing urbanization, the operational issues are increasing which in turn affect the quality of services offered to the citizens. Various government agencies provide multipleservices to the citizens. These agencies function in silos and provide a wealth of informationwhich can be utilized for efficient services across the city in making decisions anticipating the problems and by ensuring cross-agency responsive actions to the issues with fasterturnaround time.

Integrated Operation Platform (IOP) involves leveraging on the information provided byvarious departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. IOP shall be a fully integrated portal-based solution that provides seamless incident – response management, collaboration and geo-spatial display.

IOP shall provide real-time communication, collaboration and constructive decision makingamongst different agencies by envisaging potential threats, challenges and facilitatingeffective response mechanisms. Thus, the Integrated Operation Platform (IOP) provides aCommon Operating Picture (COP) of various events in real-time on a unified platform with the means to make better decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.

IOP solution should be capable of seamless integration to various government and emergency services such as law enforcement, disaster and emergency services, utility services etc., the proposed solution should support recording of external mobile video feeds, data communication, telephony etc., it should support scenario reconstruction and analytics capabilities with event timelines. The solution should support event logs including operator's onscreen activities, voice & video events etc, for further analysis, training and similar activities.

Built in analytical tools provide real-time analysis of individual events and also a measure ofthe incidents for each of the silos integrated on the platform. These help the decision makers with the in-situ challenges and facilitate immediate responsive actions to mitigate / control multiple complex challenges.

Under the Aurangabad Smart City initiative phase -1 , it is intended to cover various disparate systemsincluding:

- City Wi-Fi
- Smart Lighting
- Smart Bus Stop
- Digital Display Signages
- CCTV based City Surveillance
- ICT enabled SWM
- Biometric Attendance
- E-Governance
- GIS Application
- SMS/e-mail gateway
- IBMS
- Smart/Utility Poles
- Sensors of all types

However, the platform shall support adding more layers of solutions seamlessly with minimal effort which purchaser intends to develop in time to come. On the Integrated Operation Platform (IOP), the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on ASCDCL 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 thesystem and to impart necessary training to the users IoT Platform - Functionality

Data Aggregation, Normalization and Access:

a) Normalizes the data coming from different devices of same type (i.e. Different lighting devices, different energy meters etc.) and provide secure access to that data using data API(s) to application developers

   The city will be using various device vendors for various urban services. For example, in the Smart city journey of the city, various vendors of smart elements will be used for deployment and each will be generating data in their own format. This Platform should be able to define its own data model for each urban service like waste, lighting, transport, etc. and map data from different device vendors to the common data model. This way, application development and analytics applications do not need to worry about the complexity of various data formats.

b) Data from the IoT platform must be exposed to application eco system using secure APIs using API keys

c) Attributes of API key(s) must restrict / allow access to relevant data, i.e. (attributes can be like: specific domain (either lighting or waste, etc. or combination of these), RO / RW, specific to tenant (city, street within city, etc.)).

d) Platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. Agnostic to sensor technologies such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera or any other protocols /SDK API's of subsystem software.

e) Platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration. The platform should have the ability and provision to write adaptors, which interface with the sensors or sensor management software.

f) Platform should be able to access 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.

g) Platform should support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control.

GIS Map Support

System should support ESRI, Map Box, Open street etc.

a) Provides geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities

b) Calculates distance between two, or more, locations on the map

c) Locates and traces devices on the map

IOT platform shall enable online Developer Program tools

It should help produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost. The IoT platform vendor shall have technology labs via an online public facing web interface. These labs should be available 24X7.

API Repository / API Guide

- Normalized APIs should be integrated as per project requirement available for the listed domains (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:
- Vendor agnostic APIs to control Lighting functionality.
- Platform OEM should 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)

Platform upgrade and maintenance

- OEM should be able to securely access the platform remotely for platform updates/ upgrades and maintenance for the given duration
- Platform should be able to be deployed on DC/DR for disaster recovery

Platform functionality API management and gateway

Provides secure API lifecycle, monitoring mechanism for available APIs

- User and subscription management: should provide different tier of user categorization, authentication, authorization, and services based on subscriptions

- Application management: should provide role-based access view to applications
- Enabling analytics: Time shifted and real-time data available for big data and analytics
- Platform should also be able to bring in other e-governance data as i-frames in City Operations Command Centre dashboard
- All data should be rendered / visualized on command and control centre dashboard.

API Based Open Platform

- Provides urban services' API(s) to develop operation applications for each of the Urban Services domains.
- Platform should be able to provide API access based on roles and access control policies defined for each user and the key issued to that user
- MSI should have already documented different Urban Services APIs using which applications can be developed

  Sub system should be able to demonstrate existing applications that are developed using these urban services APIs
- Enables the City and its partners to define a standard data model for each urban services domain.
- Enables City and its partners to write software adaptors based on API(s) provided by device vendors and to control, monitor and collect data from field devices

Trending Service

System should provide trends in graphical representation from data sources over a period. Trends should allow to monitor and analyse device performance over time.

Policies and Events

- System should allow policy creation to set of rules that control the behaviour of infrastructure items. Each policy should be a set of conditions that activate the behaviour it provides. System should allow Default, Time-based, Event-based and Manual override polices creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.

System should provision to define a set of conditions that can be used to trigger an event-based policy. Visualization Layer

OCC Operations

Solution should be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.

- Solution should have the capability to integrate with GIS

- Solution shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
- Solution should provide operators and managers with a management dashboard that provides a real-time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.
- Solution shall provide the “day to day operation”, “Common Operating Picture” and situational awareness to the Centre and participating agencies during these modes of operation
- 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
- Shall provide a uniform, coherent, user-friendly and standardized interface
- Shall provide possibility to connect to workstations and accessible via web browser
- Dashboard content and layout shall be configurable, and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard
- Solution should allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes
- Shall be possible to combine the different views onto a single screen or a multi-monitor workstation. All the video management user functionalities shall be accessible directly from ICCC platform. ICC shall allow live, playback, alarm, presets etc from same GUI.
- Solution should maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system
- Solution should provide ability to extract data in desired formats for publishing and interfacing purposes
- Solution should provide ability to attach documents and other artefacts to incidents and other entities
- Solution is required to issue, log, track, manage and report on all activities underway during these modes of operation:
    - recovery
    - incident simulation

Integration capabilities

Platform shall also be able to integrate, connect, and correlate information from IoT Platform and other IT & non-IT systems, providing rule based information drawn from various sub-systems for an alert. Platform should support on the fly deployment of Sensors/IoT Devices. Platform shall have the ability to add / remove sensors including new vendor types without a need for shutdown.

Notifications, Alerts and Alarms

System should generate Notification, Alert and Alarm messages that should be visible within the Dashboard and the Field Responder Mobile App if required.

- All system messages (notifications, alerts and alarms) should always be visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
- Systems should deliver message to a set of subscribers. The Notification service should support min two types of notification methods – Email notification and Short Messaging Service (SMS) notification.

Users and roles

Users access the platform to perform various tasks, such as adding new locations, configuring new devices, managing adapters etc. Each user should be associated with one or more roles and each role is assigned a certain set of permissions.

- Platform should allow different roles to be created and assign those roles to different access control policies.
- Platform should allow single or multiple users to view and manage alarms in defined areas/Locations. User can be part of Single or multiple Areas/Locations.

Reports

Platform should have capability to provide access to real time data and historical data from various connected devices for reporting and analytics. System should have ability to generate reports and have provision to add reports in favourites list.

- Ability to display report on monitor and print report.
- Ability to capture Operators response in Text, Audio & Video
- Ability to select information to be included in report at time of report generation.
- Details of alarm including severity, time / date, description, and location.
- Map of surrounding area associated with alarm.
- Capture the operator response by text, audio & video
- Allow operator to transfer the incident report to Mobile Device/another operator’s console

Standard Operating Procedure

Software should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.

- Users should be able to edit the SOP, including adding, editing, or deleting activities.
- Users should be able to also add comments to or stop the SOP (prior to completion).
- There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
- SOP Tool should have capability to define the following activity types:
  - Manual Activity - An activity that is done manually by the owner and provide details in the description field.
  - Automation Activity - An activity that initiates and tracks a work flow and select a predefined flow order from the list.
  - If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
  - 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.
  - SOP Activity - An activity that launches another standard operating procedure

Analytics Engine

Analytics Engine should be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.

- Solution should be flexible to integrate with other city and government software applications.
- Analytics Engine module should have below intelligence capabilities;
  - Advanced Predictive Analytics should be part of the solution.
  - Solution should be flexible to integrate with other city and government software applications

  - Solution should be able to predict insights consuminghistorical data from city infrastructure viz., Traffic, Parking, Lighting etc.
  - Solution should be able to predict and integrate with Smart City solutions helping in driving operational policies creation.
  - Solution should have a visualization platform to view historic analytics
- Application should enable the operators to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks:
  - Connect to a variety of data sources
  - Analyse the result set
  - Visualize the results
  - Predict outcomes
- Analytics Engine should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel, NoSQL, RDBMS
- Analytics Engine should provide analysis of data from a selected data source(s).
- Analytics engine should provide capability to check analysis with multiple predictive algorithms
- Analytics Engine Visualizations - Analytics Engine should provide visualizations dashboard.
- In the visualization workspace, it should allow to change visual attributes of a graph.
- User should not be allowed to alter the graph/visualization definition.

API & Interface Security

- Access to the platform API(s) should be secured using API keys.
- Software should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.
- Should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where OCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.
- Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses

I. Business Operations Audit & Logging

Platform should support centralized logging & auditing framework.

- Legal / Supplier chain agreements: Platform provider vendor should have policies and procedures established, and supporting business processes and technical measures implemented, for maintaining complete, accurate and relevant agreements (e.g. SLAs) between providers and customers
- Critical production assets: Platform vendor should maintain complete inventory of critical production assets. Asset could be defined as source code, documents, binaries, configuration data, scripts, supplier agreements, SW Licenses

Field Responder Mobile

Apps provide Integrated Mobile Application for capturing real-time information from the field response team using Mobile- Standard Operating Procedure. Overall Integrated Operations Platform should account for below solution components, which can be extended to Multi-tenancy architecture;

- City Tenant activation license with one lakh device connection
- Integration of various for sensors, applications/systems as per city requirements
- Operator Client License min 25 with one city activation license

Use cases OCC and CCC Implementation

An indicative list of use cases as per Annexure which the MSI will be required to implement as part of the OCC and CCC system are detailed out below. As and when the system expands and more applications get added the MSI is required to be open to all such subsequent additions.

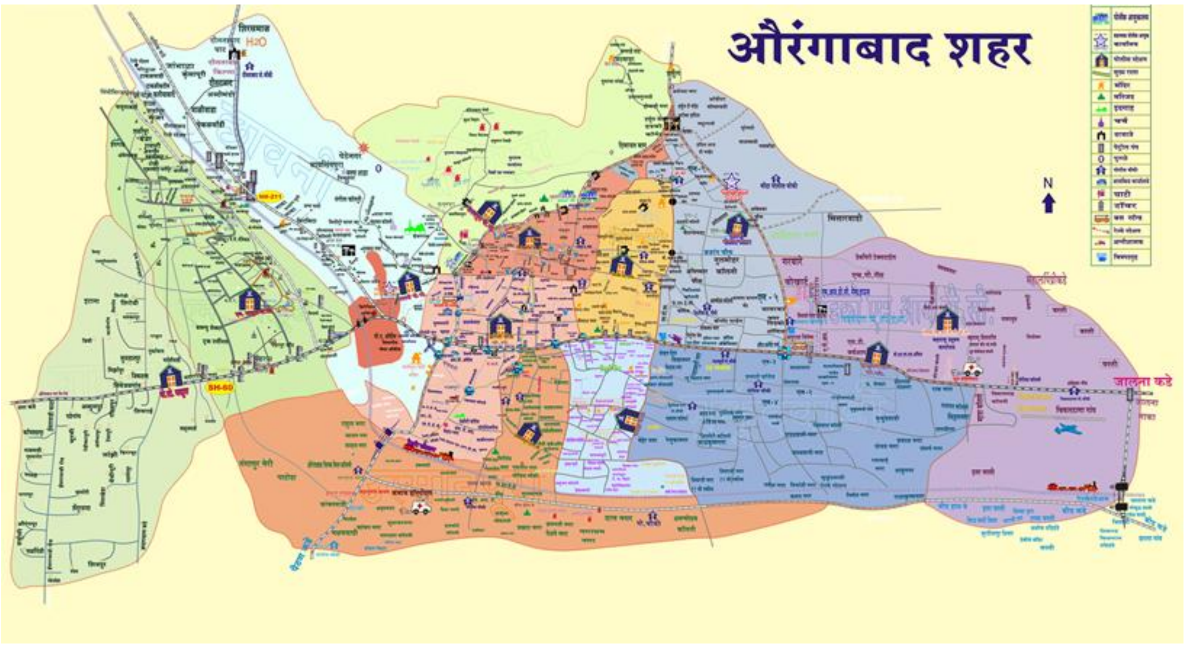
2.4. COMPONENT 4: CCTV based City Surveillance System

A. Overview

Protecting citizens and ensuring public safety is one of the topmost priorities for any Government. It requires advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, acts of violence, and all other forms of crime. CCTV based video surveillance is a security enabler to ensure public safety. Under smart city initiative, ASCDCL intends to implement a holistic City Surveillance System in Aurangabadincluding traffic enforcement system.

Geographical Spread

Aurangabad City covers an area of about 170 Sq. km. The following map represents the Geographical spread of area and zone wise distribution of police jurisdictions within the Aurangabad Municipal Corporation limits.



Aurangabad Municipal Corporation Map

B. Scope of Work

Surveillance System Infrastructure at Field Locations

This Component covers planning & implementation of the Surveillance system comprising cameras and other field equipment at identified locations. Actual placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras to ensure maximum coverage shall be done in consultation with Aurangabad Police Department.

A detailed survey shall be conducted, by the MSI along with a team of ASCDCL and Aurangabad police, at each of the strategic locations. This survey shall finalize the position of all field equipment and the orientation/ field of view of the cameras. Appropriate field of view snapshot shall be taken by a handheld camera for future reference at the time of survey. The surveyors shall also finalize the approximate location of foundation for junction box and camera poles.

The route for all the underground cable laying shall be finalized during this survey (wherever required). Every detail, finalized during the survey, shall be demarcated on an AutoCAD drawing by the SI and submitted to Purchaser in the form of a detailed site survey report along with other details for its approval.

System shall provide inter-operability of hardware, operating system, software, networking, printing, database connectivity, reporting, and communication protocols. SI shall prepare the detailed report for field level requirements e.g. Cameras (types & numbers), Camera Mounting requirements, Power Requirements, Connectivity Requirements etc. for perusal of Purchaser. Indicative list of the field level hardware to be provided by SI is as follows:

- Cameras (Fixed Box Cameras, PTZ Cameras, ANPR cameras etc.)
- IR Illuminators
- Local processing unit for ANPR / RLVD cameras
- Switches
- Outdoor Cabinets
- Pole for cameras / Mast
- Junction box
- UPS
- Networking and power cables and other related infrastructure

The indicative list of locations for the camera installation is mentioned in Annexure in the RFP document along with minimum technical requirements of associated hardware to implement a complete Surveillance system.

Supply & Installation of CCTV Surveillance Infrastructure:

Based on detailed field survey as mentioned above, MSI shall be required to supply, install and commission the surveillance system at the identified locations and thereafter undertake necessary work towards its testing.

MSI shall use industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes. Some of the check-points that need to be adhered to by the MSI while installing / commissioning cameras are as follows:

- Ensure surveillance objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey
- Ensure camera is protected from the on-field challenges of weather, physical damage and theft.
- Make proper adjustments to have the best possible image / video captured.
- Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
- Collusion preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.
- Smartcity ASCDCL brandingand/or colour coding (Police/Purchaser Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.

Installation of Poles/Cantilevers/Gantry

- MSI shall ensure that all installations are done as per satisfaction of Purchaser.
- For installation of variable message system (VaMS), CCTV Cameras, PTZ Cameras, public address system, etc. MSI shall provide appropriate poles & cantilevers and any supporting equipment.
- MSI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
- MSI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically
- 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 camera shall be made to prevent birds from sitting on top of camera box.
- The poles shall be installed with base plate, pole door, pole distributor block and cover.

- Base frames and screws shall be delivered along with poles and installed by the MSI.
- 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.
- 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 Variable Messaging Sign boards
- MSI shall provide structural calculations and drawings for the approval of Purchaser. The design shall match with common design standards as applicable under the jurisdiction of purchaser/authorized entity.
- MSI shall coordinate with concerned authorities / municipalities for installation.
- Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.
- MSI shall ensure that physical look of the installation area returns to neat & tidy conditions 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.

UPS for field locations

- UPS shall serve as a backup for commercially available utility power at the intersections and shall ensure no-break functioning of all field components at each intersection in event of failure of utility power supply.
- MSI shall carry out a study and identify locations to provide UPS backup, depending upon power situation across city, to meet the camera uptime requirements.
- MSI shall install UPS at the identified intersections in secure, tamper-proof housing in corrosion resistant cabinets.
- MSI shall ensure that the UPS is suitably protected against storms, power surges and lightning.
- MSI shall provide UPS for efficient heat dissipation without air conditioning. It shall be able to withstand temperatures prevalent in Aurangabad throughout the year.

Outdoor Cabinets / Junction Boxes;

- Each intersection shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate enforcement systems and traffic surveillance systems as defined in this RFP.

- MSI shall reserve additional room in the intersection controller cabinet to accommodate the future system requirements
- 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. Boxes shall be dustproof and impermeable to splash-water. They shall be suitable for Aurangabad 's environmental conditions. They shall have separate lockable doors for:

    a) Power cabinet: This cabinet shall house the electricity meter, online UPS system and the redundant power supply system

    b) Control cabinet: This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, RLVD, Fixed cameras etc.

- Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
- The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
- Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters 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.
- MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Aurangabad City throughout the year.

Annexure -Sample Design gives expected design guideline

Civil and Electrical Works

- MSI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:
  a. Preparation of concrete foundation for MS-Poles & cantilevers
  b. Laying of GI Pipes (B Class) complete with GI fitting
  c. Hard soil deep digging and backfilling after cabling
  d. Soft soil deep digging and backfilling after cabling
  e. Chambers with metal cover at every junction box, pole and at road crossings
  f. Concrete foundation from the Ground for outdoor racks
- MSI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, if applicable.
- MSI shall carry out all the electrical work required for powering all the components of the system
- Electrical installation and wiring shall conform to the electrical codes of India.
- MSI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup as defined in this RFP,
- For the wired Box cameras, MSI shall provision for drawing power through PoE (Power over Ethernet), while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable.
- Registration of electrical connections at all field sites shall be done in the name of ASCDCL as agreed and finalized in the contract agreement.
- MSI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

Earthing and Lightning Proof Measures

- MSI shall comply with the technical specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying. MSI shall describe the planned lightning-proof and anti-interference measures in their technical bid.
- Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables.

- All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS chip due to the surge suppression.
- Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards.
- The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized

Miscellaneous

- ASCDCL shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. MSI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. MSI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/ legal fees shall be applicable to ASCDCL for obtaining the necessary permissions. These shall be provisioned for by MSI in their financial bid.
- The MSI shall provide all material required for mounting of components such as cameras, VaMS and other field equipment. All mounting devices for installation of CCTV cameras to enable pan and tilt capabilities shall be included in the costs of the respective component. The same is also applicable to crossheads and cross arms, mounting brackets, stainless steel bands, screws and other accessories.
- All the 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 SI to be responsible to bear all cost of parts, labour, field service, pick-up and delivery related to repairs, corrections during the Project Period or any and all such incidental expenses incurred during the warranty period.
- MSI shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment / components installed under this project.
- MSI shall ensure all the equipments installed in the outdoor locations are vandal proof and in case the equipment gets damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Purchaser. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.

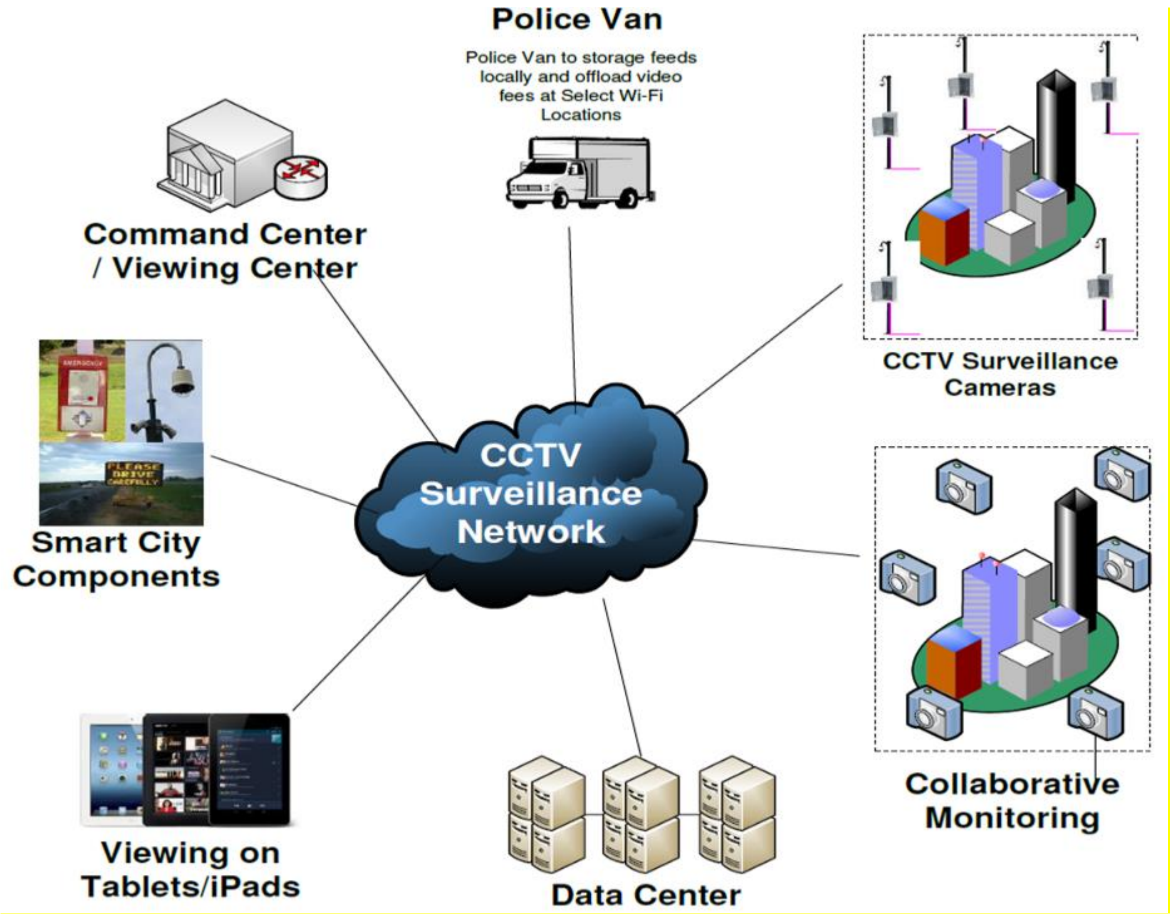
- Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and when calls are placed by ASCDCL or its designated agency.
- MSI shall be responsible for operations and maintenance of all the supplied and installed equipment's during the entire O&M phase.
- In addition to above, MSI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system.
- During implementation, if observed that any camera / field equipment requires change in the field of view / orientation, it shall be done by SI without any extra cost.
- In case of request for change in location of field equipment post installation, the same shall be borne by Purchaser at either a unit rate as per commercials or a mutually agreed cost.

C. Solution requirements

MSI shall be responsible for Supply, Installation, Implementation and Operation & Maintenance of Aurangabad CCTV based Surveillance System for a period of five (5) years from the date of Go Live. The standards should (a) at least comply with published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards.

The city-wide surveillance CCTV cameras installed in the field across Aurangabad city will help in monitoring and managing crime and enforcing traffic regulation. The CCTV cameras will, PTZ, Fixed, VaMS, FRS, Environmental Sensors, etc. Types of cameras will be installed at various locations as per Annexure 3. Local Police station should have dedicated feed from all camera in the area for local monitoring, ON demand secure access of camera viewing to mobile equipments, VAN or any authorised vehicles

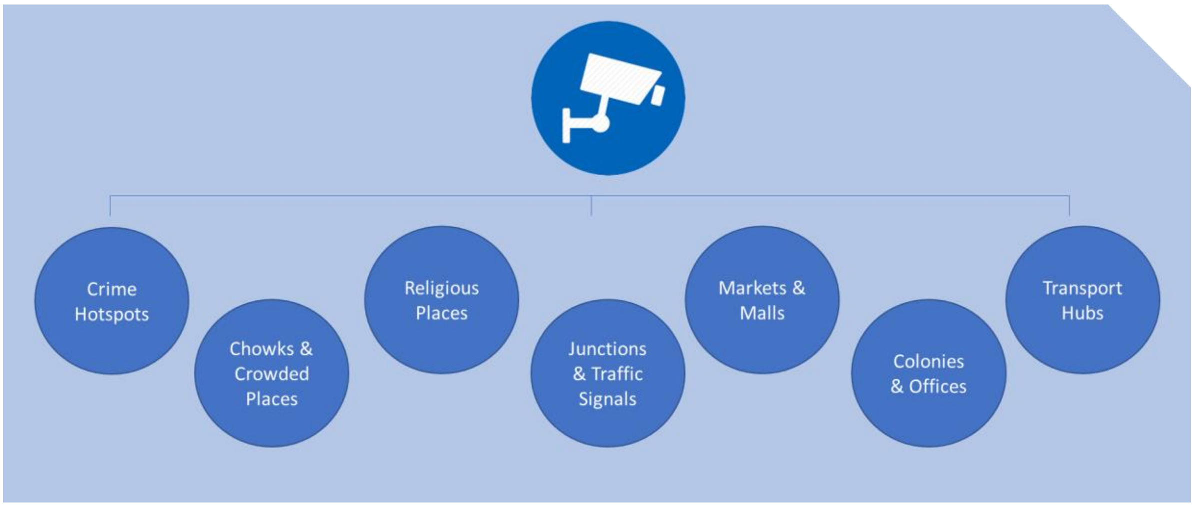
System Architecture:


Police Van
Police Van to storage feeds locally and offload video fees at Select Wi-Fi Locations
Command Center / Viewing Center
CCTV Surveillance Cameras
Smart City Components
CCTV Surveillance Network
Collaborative Monitoring
Viewing on Tablets/iPads
Data Center

To implement holistic and integrated video surveillance system in Aurangabad. The major stakeholders of CCTV surveillance system will be Aurangabad Municipal Corporation and Aurangabad Police Department. The system will help to:

- Support police to maintain Law and Order
- Act as an aid to investigation
- Improve Traffic Management
- Help in deterring, detecting and thus dealing with criminal activities
- Address threats from Terrorist attacks
- Attain faster turnaround time for crime resolution and proper investigation
- Monitoring of suspicious people, vehicles, objects etc. with respect to protecting life and property and maintaining law and order in the city
- Continuous monitoring of some vital installations/ public places in Aurangabad area for keeping eye on regular activities & for disaster management support
- Use CCTV images to ensure Public Dustbins are empty and littering

- CCTV video surveillance system will enable the above by following:
  - Providing alerts/ feedback to the Police Department about abnormal movements/ suspicious objects etc.
  - Better Management of Security breaches based on alerts received from system
  - Improved turnaround time in responding to any investigation case, faster access to evidence in case of security breach, law violation in the prescribed areas shown below as part of collaborative monitoring.



Video Management System

Video Management System (VMS) shall bring together physical security infrastructure and operations and 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. This shall allow operations managers and system integrator to build customized video surveillance networks that meet their exact requirements. Software suite shall be a scalable and flexible video management system that could be easily managed and monitored. Scalable system shall permit retrieval of live or recorded video anywhere, anytime on a variety of clients via a web browser interface.

Video management server, on which the VMS is hosted upon, shall run seamlessly in the background to manage connections, access and storage. Video management server shall accept the feed from IP Camera installed at field locations. Server shall stream incoming video to a connected storage. VMS shall support video IP fixed colour / B&W cameras, PTZ / Dome cameras, infrared cameras, low light/IR cameras and any other camera that provides a composite PAL video signal.

VMS shall facilitate situational awareness of the on-ground condition at Command Control Centre or any other view Centre. This shall be achieved by transmission of real time imagery (alarm based or on-demand). This imagery can be viewed live by operators and/or recorded for retrieval and investigation. Major functionalities are described here:

- VMS shall support a flexible rule-based system driven by schedules and events.
- VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
- VMS shall support IP cameras of different makes.
- All the offered VMS and cameras shall have ONVIF compliance.
- VMS shall be enabled for any standard storage technologies and video wall system integration.
- VMS shall be enabled for integration with any external Video Analytics Systems.
- VMS shall be capable of being deployed in a virtualized environment without loss of any functionality.
- VMS server shall be deployed in a clustered server environment for high availability and failover.
- All CCTV cameras locations shall be overlaid in graphical map in VMS Graphical User Interface. Camera selection for viewing shall be possible via clicking in the camera location on graphical map. Graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
- VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
- VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
- Whilst live control and monitoring is the primary activity of the Operator workstations, video replay shall also be accommodated on the GUI for general review and also for pre-and post alarm recording display.
- Solution design for VMS shall provide flexible video signal compression, display, storage and retrieval.
- All CCTV camera video signal inputs to the system shall be provided to command control Centre, and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
- VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or DAT tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
  - AVI files
  - Motion- Joint Photographic Experts Group (M-JPEG)
  - Moving Picture Expert Group-4 (MPEG-4)

- All streams shall be available in real-time (expecting for acceptable network latency) and at full resolution. Resolution and other related parameters shall be configurable by administrator to provide for network constraints.
- VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following minimum settings, the specific settings shall be determined according to the encoding device:
  - Brightness/Contrast
  - Colour/ Sharpness
  - Saturation/ Hue
  - White balance
- VMS shall support the following minimum operations:
  - Adding an IP device/ Updating an IP device
  - Updating basic device parameters
  - Adding\Removing channels
  - Adding\Removing output signals
  - Updating an IP channel/ Removing an IP device
  - Enabling\Disabling an IP channel
  - Refreshing an IP device (in case of firmware upgrade)

- VMS shall support retrieving data from edge storage. When a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.
- VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
- VMS shall be capable of intrusion detection: Detection of moving objects in selected areas covered by the camera (those that are specified as restricted areas like those before some major events, etc.). Avoid false alarms due to wildlife or other moving objects (e.g., tree leaves).
- VMS shall be capable of tracing of a specific person / missing child on the basis of attribute like gender, type and colour of clothes including its current full body image in multi-camera videos: Track a specific person across several surveillances (e.g., to trace and identify criminals and/or anti-social elements) on the map such functionality should be available for 50% of fixed cameras
- VMS shall be capable of counting of people and detection of abnormal crowd behaviour: Detection of people flow and counting of people in selected areas. To identify abnormal crowd behaviour and raise alarms to avoid untoward incidences in public places, and maintaining law & order.
- VMS shall allow the administrator to distribute camera load across multiple recorders and shift the cameras from one recorder to another by simple drag and drop facility.
- VMS shall support automatic failover for recording.
- VMS shall support manual failover for maintenance purpose.

- VMS shall support access and view of cameras and views on a smartphone or a tablet
- VMS shall support integration with other online and offline video analytic applications.

VMS Core Components:

- CCTV Camera Management: enables management of cameras associated with VMS.
- Video recording, retrieval and archiving: manages live camera viewing, recording of live feeds for future review, search and retrieval of recorded feeds and archiving of recorded video feeds for optimum utilization of resources.
- Security and Roles: manages role definitions for internal & external access.
- VMS should support 128 k bit encryption for recordings for security purpose

VMS General:

- VMS shall be Codec and IP camera agnostic such that it can support devices that are not supplied by manufacturer/developer of VMS software and Codec hardware.
- Each camera shall be identified by giving it a alphanumeric unique ID followed by text description field.
- When viewed on GIS map, text description of each camera shall be capable of being positioned anywhere on the monitor screen, on a camera by camera basis, shall afford options for size variations, and display with a flexible solid, semi-transparent or transparent background.
- VMS shall support tamper detection for all cameras to warn of accidental or deliberate acts that disable the surveillance capability.
- For alarm interfacing requirements, VMS shall allow selection of minimum five (5) cameras per single alarm source. The designated primary camera shall be automatically displayed as a full-screen image on the main GUI CCTV screen. VMS shall also, on alarm, present associated pre/post event video allowing the Operator to assess the alarm cause. Other associated cameras, when called up, shall be displayed as split-screen images on the other monitor of the operator workstation.
- Playback of any alarm related video, (including pre and post alarm video) shall start at the beginning or indexed part alarm sequence.
- Video management software shall incorporate online video analytics on live video images. It shall include the following video analytics detection tools:
  - Presence detection for moving and stopped vehicles
  - Directional sensitive presence detection
  - Congestion Detection
  - Loitering detection

  - Improper Parking
  - Camera Tampering
  - Abandoned objects detection
- Off-Line Video Analytics should allow for quick retrieval of video footage to metadata stored with each image. System should provide results within few seconds, system should support for below listed user's query.
  - System should allow to specify the following search criteria:
    i. Motion in the zone, user-defined with any polyline
    ii. Detection of crossing a virtual line in a user-defined direction
    iii. Loitering of an object in an area
    iv. Simultaneous presence of a few objects in an area
    v. Motion from one area to another.
  - System should support to apply below listed filters to search results:
    i. Object size
    ii. Object color
    iii. Direction of object motion
    iv. Speed of the moving object
  - Defined area entry/appearance and zone exit/disappearance
- Video clips of specific events via Video Analytics or by operator action shall be capable of being separately stored and offloaded by operator with appropriate permissions on to recordable media such as CD or Write Once Read Many (WORM) together with any associated meta-data for subsequent independent playback.
- System shall provide the capability to select duration and resolution of storage by camera, time and activity event and user request. Frequency/trigger of transfer shall be configurable by user.
- System shall provide the capability to digitally sign recorded video.
- Live video viewing: System shall allow the viewing of live video from any camera on the system at the highest rate of resolution and frame rate that the camera shall support on any workstation on the network.
- Recorded video viewing: System shall allow the viewing of recorded video from any camera on the system at whatever rate the camera was recorded.
- Storage of video: System shall store online thirty (30) days of video for all cameras on SAN/NAS storage
- 600 cameras recording @ 30 days @ HD 1080P @ Mini. 3 Mbps.
- 100 Cameras recording @ 30days @ 5MP @ min 8 Mbps.
- Incident related flag data shall be retained for additional 90 days, flagg data to be consider to be minimum of 5% of total storage.
- Competent authority will review the flag data every 30days and will decide to archive some of it to secondary storage i.e Externa HDD / USB Base Drive or allow the over writing of same.
-

- System shall provide the capability to manage the video storage to allow selective deletions, backups, and auto aging.
- VMS shall have an extensive reporting capability with ability for administrator to define reports in a user-friendly manner. The pre-existing reports shall include, but not limited to, the following:
    - Reports on alerts received by type, date and time, location
    - Reports on system errors and messages
    - Reports on master data setup including cameras, decoders, locations
    - Reports on cameras health check
    - Reports on audit trails such as user actions
    - Reports on system health including storage availability, server performance, recordings

VMS GUI Capabilities:

- User interface shall be via a GUI providing multiple video streams simultaneously on multiple monitors.
- GUI shall have the minimum capability of naming locations, users, and cameras, so that events be displayed correctly on user’s screen.
- System shall have the capability to store and record operator specific options, such as screen layout, video layout, action on alarm, and automatic video transmission settings on events.
- GUI shall conform to standard Windows conventions.
- System shall provide unified GUI camera control at an operator's workstation for all types of cameras installed whether existing or new or connected via another agency. By means of this unified control the following functions shall be provided:
    - Selection
    - Display
    - PTZ
    - Setup and adjustment
    - Determination of pre-sets
    - Any other commissioning and camera setup activity
- All user interfaces shall support English Language and shall confirm to standard Windows protocols and practices and allow the control of all functions via a simple easy to use interface.

VMS Map Functionality:

- System shall support a mode of operation whereby a map of all or part of the map (at operator request) is displayed on a separate or same screen and that status information can be provided via an icon, and access to any cameras shall be accessible by means of an icon on that screen.
- These Maps shall be defined so that an operator may select from the same source

of mapping that is available to the other systems within the command control Centre, displaying whichever Map or section the operator needs, and it shall be displayed within one (1) second.

VMS Configuration:

- VMS shall include a configuration facility to provide system administrators with a single interface utility to configure all VMS operating parameters.
- Configuration tool shall support multiple concurrent users of the system, providing the ability to automatically update. It shall also allow the codec and camera configurations to be imported and exported in excel format.
- Import/export tool shall be as sophisticated as necessary to support the following:
  - Log every action so an audit or report can be completed
  - Only update & log configurations where there is a difference between the system configuration and the new configuration file to be loaded
  - The import configuration file can contain any amount of data
  - Ability to run an update on the fly i.e. no or minimal system downtime
  - Not require a reset or restart after any upgrades
  - Definable update times
- VMS configuration tool shall define:
  - Cameras (whether via codec units or directly connected IP cameras) and text based names
  - Camera Groups / User Groups
  - Monitors / Codec parameters
  - Alarms
  - Workstations/ Storage
- Configuration utility shall allow the system administrator to:
  - Install new devices
  - Configure all aspects of existing devices
  - Configure and set up users/user groups and their rights/ permissions/ priorities
  - To define multiple camera groups
  - Each group to be defined for combinations of viewing and control rights
  - Individual Operators to be assigned multiple groups
  - Each group to be allocated to multiple Operators
  - Each camera may be in multiple groups
  - To program macros for individual and group camera characteristics
  - Program camera/monitor selection and configuration of the video wall(s) in response to an incoming alarm
  - Designate workstation destination for picture presentation in response to alarm initiation
- User permissions/privileges, to be allocated, shall extend from full administrator

rights down to basic operation of system, and shall include the ability to designate workstations to an operator, and to designate one or more camera groups to an operator for viewing and/or control.

- Configuration utility shall store all changes to system, including but not limited to:
    - User log-ins /User log-offs
    - Human interface device inputs (key strokes)
    - External alarm commands/ Error messages
- A copy of system configuration shall be stored external to the system to allow system restoration in case of hardware failure.

VMS User Hierarchy:

- MSI shall request a detailed User Prioritization List (UPL) during the project.
- UPL shall enable programming of CCTV management system with agreed user prioritization.
- Over and above user priority, users shall be enabled for following in varying combinations:
    - Image viewing
    - Image recording
    - PTZ control
- In addition, control location shall be prioritized such that command control Centre has full control of all functions and priority one override over all other locations.
- Within the hierarchy, each user's log-on password shall not only allow access to varying levels of system functionality, but shall provide for relative priority between users of equal access rights. Operators in above groups shall be individually allocated a priority level that allows or denies access to functions when in conflict with another operator of lower or higher priority level.
- These priority levels and features they contain shall be discussed and defined with the system administrator. MSI shall allow time to carry out this exercise together with relevant configuration of groups, sub-groups, permissions and priorities.

VMS Recording Requirements:

- All images shall be recorded centrally as a background process at configurable parameters.
- It shall not be possible to interrupt, stop, delay or interfere with the recording streams in any way, without the appropriate user rights.
- CCTV recording system shall enable Pre and Post Event (PPE) recording, presentation and storage, initiated automatically in response to system alarm sources received by the VMS.
- PPE recording clips shall be provided by the VMS and retrieved from the central video archive on the buffer storage system. This PPE stream shall be totally

independent of the background recording stream provided to the central video archive such that central video archive recording, as programmed, continues under all circumstances.

- Information stored shall be full real-time and full resolution from each incoming camera channel. In the absence of a trigger from a manual input or from a programmed alarm source, the PPE video recording shall be written to buffer storage on a FIFO basis.
- PPE periods initiated by a single alarm occurrence shall be configurable via the VMS as follows:
    - Pre – 0 to 30 seconds
    - Post – 30 to 300 seconds
    - Shall be variable for each camera according to each individual alarm and the alarm type
- In the event of a trigger, VMS shall ensure that the programmed sections of pre and post event video are immediately presented to the Operator to complement alarm display and simultaneously saved as an identified indexed video clip, complete with time/date stamp, in a reserved and protected area of storage system. Such PPE recording shall then be capable of retrieval via search criteria.
- Once tagged and saved, the PPE video clip shall NOT be overwritten except by an operator with the required permissions i.e. it is excluded from the normal FIFO regime of the bulk storage system. Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stoke.
- VMS shall support the following recording modes:
    - Total recording - VMS shall constantly record video input. VMS shall allow for continuous recording of all video inputs
    - Event based recording - VMS shall record video input only in case an event has occurred
- VMS shall support following triggers to initiate a recording
    - Scheduler - recorder will record video inputs based on a specified schedule.
        - VMS shall allow recording based on a time schedule for all or some video channels
        - VMS shall allow for multiple recording periods per day, per channel
        - VMS shall have option to set any available trigger in the system (VMD, TTL and/or API) to trigger the channel
        - VMS shall have option for individual channel setup of pre/post-alarm recording for defined interval (e.g. up to 10 minutes pre-alarm and 30 min post-alarm recording)
        - VMS shall have ability to enable/disable triggers through a daily time schedule
    - Manual - user shall be able to initiate a manual recording upon request

  - VMS shall work in conjunction to the any previous alarm operations
  - VMS shall allow API Triggers
  - All trigger information shall be stored with the video information in the VMS data set and shall be made available for video search

Manual or on demand recording:

- Recording shall also be initiated on-demand by manual triggers from system operators e.g. keyboard key-stoke (subject to user rights).
- System shall allow for an operator to initiate recording on any live stream being viewed.

VMS review system: VMS recording and replay management systems shall support the following features and operations:

- Play back shall not interfere with recording in any way
- Support either analogue cameras connected via Codecs or IP-cameras directly connected to the network
- Stream live images through the network using IP Multi-cast techniques
- Stream images from the Codec to the attached storage system
- Store the recording stream from all cameras simultaneously with no degradation to any individual camera recorded image stream unless the system is configured by administrator to allow for change in quality
- Deliver live video to VMS workstation within a period of one second from manual call up
- Deliver live video to VMS workstation within a period of three seconds from automatic alarm receipt on alarm interface
- Storage of each camera’s images at a rate and resolution as defined in the Codec or IP camera configuration. VMS programming shall automatically vary these rates in response to time profiles, alarm inputs
- Support multiple, configurable recording time schedules per camera. Each schedule shall support different recording parameters and automatically implement against configured time schedule e.g. operational and non-operational hours shall be scheduled with different recording parameters on designated cameras
- Support streaming of recorded files using IP Unicast directly to hardware decoders for display on analogue monitors or software decoder when/if required
- Playback multiple, synchronized recorded streams at differing speeds and frame rates
- Record and playback a video stream simultaneously at differing speeds and frame rates
- Time stamping of every recorded video field based upon Network Time Protocol (NTP) time

- Selectable on-screen-display of time and camera title during playback
- Security file lock to prevent specific recorded files from being overwritten regardless of their date and time, in addition to those records stored as PPE clips. The duration and policy for retention of such videos would be same as that of the PPE clips
- Configurable granularity of video files
- Generate alarm when storage medium has fallen below a user selectable threshold
- Stored video files can be "downloaded" directly to DVD or WORM for replay using VMS video replay application and shall incorporate proof of authenticity
- Download video records in common (e.g. AVI) file format for remote, cursory review and assessment prior to generating tamper-evident auditable copies
- The VMS client shall support LoS (Level of Service) mechanism, choosing between several video streams according to its performance parameters and networking capabilities of the workstation and/or decoder to be able to decode more cameras.

VMS Alarm Handling:

- Video alarm handling shall provide following facilities for handling and management of video images generated by alarms associated with other systems integrated with VMS.
- Whilst pre and post alarm requirement has been included (up to thirty (30) seconds) pre alarm, three hundred (300) seconds post alarm per camera at fifteen (15) FPS, VMS shall display and manage pre and post alarm information as follows for a maximum of two hundred (200) alarms per day:
    - Pre and post alarm video clip shall be displayed full screen, in real-time and shall continuously play the 'loop' until the operator accepts the initial alarm activation or clears down the event
    - Pre and post alarm shall be displayed on a dedicated monitor
    - Each monitoring station shall be able to display simultaneous alarms
    - Video clip associated with alarm shall be tagged with date, time, etc. and stored in a dedicated location for retrieval later.
    - Alarm archived video shall be readily available for one month but accessible for six months
    - VMS shall accommodate at least 100 simultaneously alarm activating CCTV cameras
    - All alarm based images shall be displayed
- VMS shall have the capability to automatically display a primary camera, plus minimum of four additional cameras associated with each alarm based on either camera locations with respect to the alarm, or a programmed set of parameters defining the associated cameras.

- The VMS shall be able to set smart triggers combining two different trigger using OR/AND logical entities.
- Administrator shall be able to define a set of VMS operations as a macro (rule-based automatic actions). Administrator shall be able to associate the macro with one or more conditions/events that are related to incidents, sensors (including video cameras, ACS, Fire, Intrusion sensors and alarm panels etc), date/time and integration gateway status
- Alarm shall include associated predefined operational workflow procedures to provide the operator structured guidance as well as assistive information for successfully managing an incident. It shall allow collaboration by involving other system users as stakeholder that can have access to the incident and contribute to the incident’s management by completing tasks and adding information to it.
- The incident shall allow communication between its stakeholders through a textual message
- VMS shall also accommodate operator-initiated recording of a given camera. The operator-initiated recording shall:
    - Accommodate up to a total of at least 50 cameras simultaneously (all operators)
    - Record the selected camera/s for an administrator configured number of hours or until stopped, whichever is the sooner

VMS Integration requirements:

- VMS shall be integrated within a consolidated GUI that would include other command control Centre systems as well. All events, activations and alarms that occur with the VMS and its sub systems will interact seamlessly between the command and control Centre sub systems as required
- Either OPC or SDK shall manage interface between VMS, GUI and other City Management systems as required.
- OPC or SDK shall allow the operator workstations to control the VMS irrespective of the vendor chosen by duplicating all control functionality of the VMS used for normal day-to-day activities.
- Alarm linking between VMS sub-systems shall be done at VMS sub-system level to, for example, call up relevant pictures to screens and move PTZ units to pre-set positions in response to alarm and activate video recordings, modifying recording parameters as necessary.
- All OPC software shall be fully compliant with the OPC specification as set down by the OPC foundation. Any software or products which are not compliant shall be highlighted in the Technical Proposal return. MSI shall indicate in the technical proposal return how the OPC interface shall be implemented.
- If an OPC interface cannot be provided, an alternative solution shall be provided for this data using a standard open protocol and confirmation as to how this shall

be implemented shall be provided in the technical proposal return.

- If an SDK solution is provided the system shall allow reconfiguration by (City) and end users without recourse to special languages. A system SDKs shall be supplied with all required supporting software to allow the integration of the system with new devices and systems.

VMS System Size:

- VMS shall enable handling of all the cameras, on day one, as well as future scalability as may be required.

Video Analytics

Surveillance system shall have capability to deploy intelligent video analytics software on any of the selected fixed cameras. This software shall have capability to provide various alarms & triggers. The software shall essentially evolve to automate the suspect activity capture and escalation; eliminate need of human observation of video on a 24x7 basis.

Analytics software shall bring significant benefit to review the incidences and look for suspicious activity in both live video feeds and recorded footages.
Minimum video analytics that shall be offered on identified cameras are:

- Presence detection for moving and stopped vehicles
- Directional sensitive presence detection
- Congestion Detection
- Loitering detection
- Improper Parking
- Camera Tampering
- Abandoned objects detection
- Unattended object
- Object Classification
- Tripwire/Intrusion
- Person search

The solution shall enable simultaneous digital video recording from network, intelligent video analysis and remote access to live and recorded images from any networked computer. It shall be able to automatically track objects such as cars and people and push content to the respective security personnel as required for real time analysis. The system shall also have display of time line, customizable site map, live video, video playback, integrated site map, remote live view, multi-site capability, encryption, watermarking and event based recording.

All cameras should support motion detection, camera tampering. All cameras must be capable to run two analytics in addition to motion detection and camera tampering as required at any given time.

Solution shall be so designed to have Automated PTZ camera control for zooming in on interesting events like motion detection etc. as picked up by camera without the need of human intervention. It shall be completely scalable, with a many-to-many client-server model allowing multiple physical systems to be used in an array of servers. The server specified in the RFP indicates only the minimum requirements. However, SI shall offer the server system to suit the video analytics requirements specified herein.

2.5. COMPONENT 5: Biometric Attendance system

A. Overview

Aurangabad Smart City Development Corporation Limited intends to implement e-Office System - Biometric Attendance Management system. ASCDCL is looking for AADHAAR enabled biometric e-attendance system, for ASCDCL office. This will help increase efficiency, transparency of governance.

B. Scope of Work

Finger Print based Attendance System

a. Supply, Installation, Commissioning & Maintenance of AADHAAR based biometric e-attendance system at specified locations of the subordinate AMC premises.

b. Supply, Installation, Commissioning & maintenance of all other active, passive components and other infrastructure for the biometric attendance system aProvide necessary support for registration of AMC & ASCDCL employees on e-attendance system.

c. Provide training to end users

The implementation of face recognition biometric attendance system will cover the Head Office of Aurangabad Municipal Corporation and finger print biometric attendance system will cover the ward offices and handheld finger print biometric attendance devices with GPS tagging will be deployed for field staff. Location as per Annexure.

Handheld Biometric Device

Supply and Installation of AADHAAR enabled Biometric E-attendance Fixed and handheld devices (for field staff) at ASCDCL office in Aurangabad, confirming to the technical specifications mentioned in the RFP. In future, if new offices are established, the MSI should supply the comparable and compatible configuration devices and carry out all the installation and integration with the existing system on mutually agreeable terms and conditions. The installed biometric device should have features as under:

Fixed Biometric Devices:

- Fixed biometric devices should be of good quality with proper display screen enclosed in a tamper proof box.
- Device should be able to operate in temperatures of 0-50°C and humidity range of 20-95%.

- Biometric devices should provide:
  - Centralized Biometric Access control on IP technology for complete enterprise
  - Centralized Server & Terminal based Fingerprint time attendance
  - 5.7 inch or larger true colour Screen LCD
  - Auto-on function & Live Finger detection
  - Built-in camera takes picture for every transaction
  - USB memory slot & Wi-Fi in addition to TCP/IP Ethernet / GSM
  - Identification time < 1 sec
  - Template capacity: 100,000 events (50,000 users)
  - 4 hour battery
- FAR/ FRR should be less than or equal to .0001%.
- Devices should be covered under warranty for at least 1 year and AMC thereon.
- Devices to be installed by creating suitable bays at each entrance for systematic biometric scanning at the AMC premises.

Handheld (HH) Biometric Devices:

- HH device should be rugged & robust enough for use in rough environment for a long period. It should be built in a tamper proof rugged body to make it more secure and rodent proof. Device should be rugged enough for field usage and weight should not be more than 350 gms. Easy to carry in field. Water and dust proof. IP 65 Certification to be provided.
- Latest High Speed Processor capable of supporting latest Android OS/ latest Linux OS. CPU Speed of 1 GHz or more; Minimum RAM 1 GB or higher.
- Flash memory of minimum 4GB upgradable up to 32 GB with SD Card holder
- Minimum 3.5 Inch Touch Screen TFT LCD 320 X 3 (RGB) X 240 pixels with sunlight readability.
- 30 Keys Alphanumeric bigger & easy to operate Keyboard
- Lithium-Polymer/Lithium –Ion with minimum 4500 mAh above suitable for minimum 8 hours operation. Life: 300 cycles.
- AC 180V to 240V charger for 3 to 4 hours charging.
- Aesthetically designed ABS or Poly Carbonate plastic Housing, with integrated, LCD display, Fingerprint sensor and Keyboard etc.

- Communication with GPRS for 4G (mandatory) with provision for at least 1 SIM Card (dual SIM will be preferred)
- Inbuilt GPS Module with minimum 30 channels, support AGPS and DGPS anti jamming, cold start time less than 40 Sec, low power consuming and provide location details within the range of 100 meters area.
- Inbuilt Speaker with 1W or above Speaker Supporting WAV Files
- Operating System - Android OS 4.2 or above /Linux OS latest version
- Data Ports - USB 2.0 & RS-232 (optional)
- Protocol - TCP/IP Ethernet / HTTP /HTTPS / GSM
- STQC certified high performance Finger Print Scanner with optical sensor (500 dpi)
- Best Finger Detection (BFD) client application conforming to Aadhaar based BFD API 1.6. BFD application should have capability of displaying NFIQ score of each finger.
- Inbuilt NFIQ quality software either at device level or extractor level. High Quality Image (NFIQ<=2) in dry, wet, dirt, oil dry and bright light conditions
- Finger Capture Device performance: Sensor shall have failure to enrolment rate (FTE) of 0.01%. Sensor shall have no or very low Failure to Acquire Rate (FTA) of 0.001%. Sensor shall be able to generate good quality image and produce high scores on recommended test procedures /standards for more than 95% of the time, for the following different field operating real world conditions.
- Audio/Visual Indication: Indication either at device level or at application level for indicating various events like: (a) Indication for placing finger. (b) Start of capturing. (c) End of capturing.
- Client side Application: Pre-loaded client side software application in Handheld devices needs to conform to the following:
    - Device Connectivity with server with multiple channels combination of GPRS (dual SIM), 3G connectivity and Device should access only the provided web services of e-POS server.
    - Client software should be able to transfer fingerprints to UIDAI Server for authentication response and perform authentication transaction.
    - Client Software should be able to handle both online & offline transactions
    - Client software should be available in English Interface with Unicode Font support. Device should be able to readout the specifics of the transaction in both the languages. The Successful MSI will ensure that HH devices

continue to operate through upgrades and new releases of software. MSI will ensure minimum interruption during upgrades to such software.

- Each authentication response time should be less than 6 seconds.

- Devices should be covered under warranty for at least 1 year and AMC thereon.

C. Solution Requirements

AADHAAR enabled finger print biometric e-attendance:

The implementation of biometric attendance system will cover the Head Office of Aurangabad Municipal Corporation and finger print biometric attendance system will cover the ward offices and handheld finger print biometric attendance devices with GPS tagging will be deployed for field staff.

This technology will help accurately track employee attendance and time. It will also eliminate cases of leaving early, arriving late or unauthorized overtime. The biometrics terminals read each employee's unique fingerprint, hand shape, iris or face shape, they ensure employees are unable to clock in for one another, preventing cases of employee time theft. This system is a convenient security solution because no passwords, no badges nor ID cards, etc are required to be carried or checked.

Deploy and run suitable Human- Machine Interface .The Human-Machine Interface shall be developed using Ergonomics of System Interaction guidelines. web-based e-attendance reports for the process requirements of AADHAAR enabled biometric e-attendance system.
Enable an enrolled user to register the Employee ID, verification, timestamping based on AADHAAR enabled biometric e-attendance system.
System shall not store biometric signatures locally except during transaction. Once the transaction has concluded all biometric data captured shall be purged.

System to be integrated in attendance.gov.in

Implementation of a web based reporting application: ASCDCL has envisaged following activities pertaining to web-based application software that are required to be taken up by MSI to achieve the objectives:

a) MIS Reports: System should support integrated MIS with following reports:

- Daily E-attendance Report
- Device wise E-attendance Report
- Time wise E-attendance Report
- Employee Check-in and Check-out Log Report

- Summary of Late coming employees
- Summary report of punctual Employees for a specified period
- E-attendance Summary Report for a month/quarter/year

b) User-based access to various e-attendance reports.

c) Database creation and Master creation with Facial and Fingerprint image registrations of AMC /ASCDCL employees

d) Integration with HRMS and Payroll systems of AMC and ASCDCL

- Manage leave, absence and late coming records
- Integrate with accounts for payroll deductions based on rules set by ASCDCL

e) Deployment shall include implementation and maintenance of the software.

f) MSI shall be responsible for creation of Master Data regarding ASCDCL employee data, their signatures etc. required for implementation of biometric e-attendance system under the supervision of Admin & Accounts Sections at ASCDCL Office.

g) Hands on Training over the web-based module:

- MSI shall provide hands on user training to the ASCDCL staff for proper functioning of biometric e-attendance system.
- Training shall be conducted for two days at ASCDCL Office.
- Training Plan shall be mutually decided between ASCDCL and the MSI.
- During training, user manuals for the web-based reporting module shall be provided by the successful MSI.
- MSI must include all cost for training, travelling, boarding, lodging cost in financial bid.
- Integration into attendance.gov.in portal for National attendance system integration.

2.6. COMPONENT 6: Smart Transport System & Smart Bus Stops

A. Overview

The planned public transport system with fleet of 100 buses. These buses will be equipped with GPS devices for automated tracking of buses. Passenger Information System will be implemented to provide real time information about buses & their schedule on a particular route to the passengers/commuters. Fleet management system will also be installed to manage the entire fleet of the buses. Similar systems will be installed on new buses which will introduced in the future

As part of Aurangabad Smart City initiatives, the aim is to make transport efficient by introducing following components.

- Smart Bus Stops with various functionalities such as VaMS, People Counter, CCTV Camera for surveillance, Wi-Fi Hotspots, Environment Sensors,On Grid Solar Panel 3KVA (125 sq ft solar panel) etc.
- Fleet Management System for AMC and/or MSRTC City Transport Vehicles
- PIS at Bus Shelters to display Schedule of buses
- PIS, Bill Boards, Wi-Fi for Smart Bus Stops
- Geo Tagging of bus routes through RF readers on bus stops and RF tags & GPS devices on buses
- Public Vehicle Tracking application to be integrated into the Citizen App

The public transport in Aurangabad has unscheduled arrivals and departures, missed trips causing lot of inconvenience to the public because of which public transport is minimally used, which results in increase in use of private vehicles thereby increasing the road traffic and vehicular pollution. The cost of private auto-rickshaw based transport is unaffordable and thus increases -Wheeler and 4-Wheeler vehicular traffic.

The solution should give ASCDCL the ability to track, record, and analyse how vehicles are performing in real time. These features will lead to improvements in public transit service through better on-time performance and quicker response time to emergencies. The location information along with other details such as the speed of bus, route followed, etc. will be used to provide the passengers waiting at the bus stops with expected arrival time of bus. The information will be displayed on boards installed at the bus stops, inside bus, websites, mobile apps, etc. The system should also help in improving the efficiency of bus operation by generating various standard and exception reports.

B. Scope of Work

Smart Transport System

- MSI shall integrate GPS based Automated Vehicle Locator System (AVLS) in city Bus and integrate with OCC
- MSI would install PIS system at the bus shelters
- MSI should integrate the AVLS on the GIS maps provided by ASCDCL
- MSI should also provide a Mobile / Web Site based information to passengers about the real-time location of bus.
- MSI should provide Passenger Information System (PIS) in the bus and also at the Smart Bus Stops.

I. Functional Specifications - Vehicle Location System & Passenger Information System

a) Ability to locate a bus at a given time in its track to estimate its arrival/departure time at the next destination, based on traffic density, distance, speed, bus occupancy, run-time information from the previous bus arrival time for the same location etc.

b) Ability to receive SOS and alerts from moving / stranded buses enroute

c) Facility to track defined vs. actual movement of vehicles, capture deviations if any.

d) Facility to view vehicle movement in a real-time mode on GIS maps provided by ASCDCL.

e) Ability to provide dynamic location specific information as the vehicle approaches bus stop/station for the benefit of passengers

f) Facility to generate information such as travel time estimation, average time at bus stop, passenger traffic at different location, alerts on exceptions, and logging of the journey details of the bus for each trip

g) Facility for citizens to access and view position / location information on GIS maps near real time through web interface with historic data displayed on maps

h) Facility for providing current information location on demand

i) It should enable operational managers to create locations, routes, schedules Vehicle service alerts for service and maintenance

j) Provide daily Maintenance Schedule, pending Insurance and pending Pollution Check status

k) Vehicle fleet summary dashboard – quick view on vehicle fleet performance based on fuel Consumption, it should provide average fuel consumed per kilometre.

l) System should also be able to record bus break down instances along with other exception recording/ actions (over-speeding, off-route detection, non- stoppage at bus stops, trip cancellation)

m) System should generate reports

- Depot, vehicle and route wise reports
- Missed stops reports
- Route deviation reports
- Trip status reports (Cut/Short/Missed)
- Distance travelled
- Register a bus on unscheduled route from backend on real time basis

II. Functional Specifications – Mobile Application

a) Real-time bus tracking system (Support 3rd party application provider)

b) Complete information on bus routes and stops to commuters

c) Real-time ETA for a combination of bus route and stop

d) Real-time tracking for the bus on the map

e) Mobile Application for IOS, Android and Windows mobile devices

f) MSI shall develop mobile apps which shall include a mobile application to help passengers to get information about the buses, search and view bus schedules on various routes and deliver ETA based on their real time location.

g) System shall show the time table of the buses, fare structure etc.

III. Module: Multi Fleet System

Functionality	Public Transport Requirements Served
Information about all running and idle vehicle with following information: Driver Name, Contact Number, Speed, Current Location, Schedule time to reach next destination, No. of trips till now, Current trip number, No. of Delayed trips, Current trip status	Multi-fleet systems: ▪ All-in and simultaneous management of several fleets. The sharing of resources (communications system, control centre and human management resources) creates beneficial economies of scale. ▪ A section which enables user to have a full view of all activities of the fleet on a single Console. The dashboard shall form part of the UI delivery which shows all key performance and tracking indicators enabling control centre staff and management team of Public Transport ASCDCL to take proactive Decision to manage Transportation operations in a highly efficient manner. ▪ Application development and customization of screens, forms, reports and queries of data specifically include: ▪ Locating a particular bus in the fleet ▪ Auto pan facility for tracking a particular bus ▪ Sending online messages to an individual bus or group of buses selected on a map

IV. Module: Live Vehicle/Real Time Tracking

Functionality	Public Transport Requirements Served
Tracking and Monitoring Bus Status (Running, Stopped, Ignition Off) Running Speed Route Source & Destination Stoppages Visited Current Location Stoppages to Visit Bus Identity, Route Identity and Name	▪ Integration of GPS with digitized map for tracking of vehicles on a real time basis including distress messaging between vehicle and control station. ▪ To monitor whether the buses are adhering to its scheduled route and time table through-out the route and identify if there are any deviation. ▪ Real time two way messaging between buses & Central Control Room. ▪ To monitor whether the buses halt at all the scheduled bus stops. ▪ Generating messages pertaining to speed violation, skipped bus stops etc., to Public Transport officials at the Central Control Station, online along with the Geo-graphical position and the violated vehicle number
Punctuality	
Current Location & Time	
Transit Diagram and ETA	
Tracking Bus Actual Transit against Scheduled Transit	

V. Module: Reports & MIS

Functionality	Public Transport Requirements Served
Different Analytical, Revenue Management and Alert reports (Through Data received from legacy Revenue Collection System)	▪ Generation of exception reports like deviation from schedule route, timing, Missing Bus stops, Punctuality factor, etc. based on captured vehicle data ▪ Calculation of actual distance (in kms) travelled by vehicle, using map ▪ Reports: o Speed Log o Stoppage Log o Summary Report Day Wise Vehicle Wise o Performance Day Wise Vehicle Wise ▪ Statistics: Monthly Performance ▪ Alerts: o Fleet Summary o Vehicle Status o Speed Violation o Real-time application data delivery for PIS
Speed Log	
Stoppage Log	
Summary Report Day Wise	
Performance Day Wise, Week Wise, Monthly	
Performance Vehicle Wise	
Summary Report Vehicle Wise	
Monthly Performance	
Calculation of actual distance (in kms) travelled by vehicle using digitized map.	
Depot Report	
Deviation from schedule route or timing.	

VI. General Functional Requirement of the proposed Application Software

a) The proposed system will be capable of data communication with all the system components in real-time.

b) Uploaded data will not be deleted from device readers or workstations until the central system has provided confirmation acknowledgement that the transactions have been successfully received

c) The proposed system will be able to update its date and time using time synchronization application of servers. Also the date and time on all system devices and workstations should also be updated

d) All active equipment will have an internally maintained date and time clock that is synchronized using a time interval via the communications medium with the system date and time clock

e) System should be driven by configurable parameters and should provide flexibility for maximum configuration. Configurations will be for, but not limited to:

- User groups and users privileges
- Time based messages/reports
- Addition & deletion of equipment's, nodes, stations, user groups, users
- Reports Access
- Configurable messages

f) System should handle all degraded conditions which can be, but not limited to the following:

- Power failures
- Data connection lost
- Central server down
- Bus-station switch non-functional

g) Software should provide controls to view the entire sequence of reported locations from the beginning of the time or to step through the sequence incrementally forwards or backwards.

- Replay data will include location and headway adherence data.
- System will allow replay for a single vehicle, selected set of vehicles or all vehicles or cluster wise vehicle or route wise vehicle on the selected map view for selected time period
- All users accessing the AVL software will be able to access the playback function.

- System will be able to store a playback in a format that can be exported for viewing on any computer.
- System will allow the ability to use playback without exiting from the current AVL operational view.

h) Software will be accessed on workstations and CCC/OCC of all users identified by ASCDCL. All communications and AVL data will be stored in a manner that allows direct access by the software for at least 120 days and reporting data for 18 months live in the system. MSI will provide Utilities to support archive and restore functions for older data.

- System will only be accessible by authorized persons, controlled using login and password protection. Single Sign On will be provided for all modules in CCC/OCC
- System will maintain a transaction log that records all users that access system reports. The pages/reports accessed, edits and changes to the database and the system logon and logoff times. The transaction log will maintain this information for a minimum of one year.

i) System will allow selection of any time for the historical data. All data will be the property of ASCDCL and will be immediately available to ASCDCL.

j) Central system shall be delivered with a fully functioning Graphical User Interface

k) Graphical User Interface shall be based on standard web based browser controls or an equivalent system

l) It shall be possible to create different user classes/categories/roles with different access level

m) System security will provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.

n) Features will be provided to ensure that all system-created files are uniquely identified, and that no files are lost or missed during data transfer.

o) System will have verification features to confirm that there have been no losses of data at any point in the transfers.

p) System needs to be tamper proof and MSI should build features to confirm that there have been no unauthorized changes to, or destruction of, data.

q) Features will be provided to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.

r) All systems, sub-systems and devices will only allow access to authorized user classes.

s) All security breach detections will be confidential, and accessible only to users of the appropriate class.

t) Web-based system and all equipment (on-board equipment, PIS displays in stations etc.) will support a maintenance mode during repair, replacement and testing of equipment.

u) All the functions that are carried out in the maintenance mode will be reported separately similar to exception transactions

v) Maintenance mode will be possible to be activated based on a particular node wise

w) Maintenance mode can be activated only by a person having the highest user privilege in terms of system operations.

x) Logins and logouts will be transmitted to the system, along with associated Date/Time, employee ID, equipment ID etc.

y) It will be possible to upgrade the firmware/ software from the central server using the internet communication available at the station level.

z) Central software will be scalable to accommodate for buses, bus-station/Smart Bus Stops/terminal PIS, without any modifications to the central software except minor configuration changes, the details of how scalable the system is will be provided in the proposal by the MSI at the time of inception report.

aa) Minimum scalability will be for 100 Buses, 100 PIS for Smart Bus stops and Bus terminal.

bb) Software will provide standard reports based on the AVL data. MSI will provide details in their proposal related to reports that are offered and the degree to which they can be configured (at minimum all report will be configurable for a specified date/time range and route). Some of the expected standard reports are as follows:

- Headway adherence
- Active fleet (weekday and weekend)
- Service hours and mileage
- Schedule Adherence
- Speed Reports
- Route Deviation reports

cc) All reports will use standard reporting tools (e.g., RDBMS or SQL or Crystal Reports etc.) and will have the ability to export data into file formats that can be exported to and edited with standard tool i.e. excel, etc. The MSI shall provide the relational database layout including related fields, key fields and definitions for all fields in all tables in the database

dd) Any portion of transactional database will be exportable in standard formats (such as comma separated variable (.CSV, xls, xlsx files etc.) for analysis in third party programs.

ee) It will be possible for users to build custom reports from the data in the transactional database with tools such as RDBMS or SQL. The reports will be capable to be exported to pdf, xls, xlsx formats easily

ff) Data dictionary will be provided to ASCDCL to facilitate development of custom reports.

gg) MSI will be responsible for the design and development of the website, including all required HTML, scripting, and integration with the AVL system. The website GUI will allow for the graphical presentation of vehicle locations on GIS-based maps.

C. Solution Requirements

One of the most important and visible portions of the Smart City will be 57 Bus-Stops of Smart City Aurangabad. This innovative structure will define the public perception of the project and increase the use of Smart Public transport. A successful implementation of Smart Bus Stops should increase the ridership on Public Transport and thereby pay for the additional cost incurred for creating this facility. Secondary benefit will be the reduction of vehicular traffic.

MSI should Design, Build, Operate and Maintain Smart Bus Stops in Aurangabad city at identified locations. These smart bus stops will be equipped with following components:

- Environmental sensors
- Public Address System
- Emergency/Panic Button
- Passenger Information System
- Outdoor LED Digital Display/ Variable Messaging System
- Advertisement Panels along with framing
- Bench with steel planters
- Lighting arrangement
- Separate dustbins for dry & wet waste
- Wi-Fi Hotspots
- PTZ Camera for Surveillance at the smart bus stops
- ON grid Rooftop Solar PV System
- Smartcity ASCDCL branding on all bus and bus stops

The existing 57 numbers of bus stops will be dismantled and replaced by specially designed and branded smart bus stops with facilities as explained in the following sections. The MSI must aesthetically and ergonomically design the bus stops with suitable branding. A sample design of the Bus-Stop has been included in the RFP as a reference.

- Dismantle existing bus shelters at existing locations and necessary site preparation for all locations
- Design and build the Smart Bus Stops aesthetically and functionally such that the Smart Bus Stops become a hallmark of the city.
- Develop and landscape the area surrounding the smart bus stops.
- Paver blocks and tactile pavers (along the walking & boarding strip) should be installed around the bus stop as per approved design.
- Ensure that all design of smart bus stops and amenities are based on the principle of universal accessible design.
- Provide general cleanliness and adequate power supply for proper lighting of the Smart Bus Stop.
- Provide and facilitate proper functioning of Passenger Information System at the Smart Bus Stops.
- Provide people counter for counting the number of people using the bus stop.
- Provide Solar PV modules with other equipment/accessories on the roof of the bus stop for generation and consumption of electricity within the bus stop. The solar PV pane should be aesthetically included in the overall design of the bus stop.
- Undertake adequate measures for safety and security of users, including deployment of security personnel and gadgets such as CCTV (PTZ Camera), etc. MSI is required to employ trained professionals to operate and maintain the Smart Bus Stop and other amenities system
- Provide structurally sound and aesthetically appealing passenger facilities such as clock, route maps, etc.
- Provide adequate and comfortable seating facilities for passengers at each Smart Bus Stop
- Design and construct a kerb to facilitate ease of boarding and alighting of passengers, particularly physically challenged and senior citizens
- Make special arrangements such as, ramps, hand rails, etc. for the differentially

abled users and the senior citizens.

- Take necessary precaution for environmental and social safeguards in accordance with applicable norms and guidelines
- Operate the Smart Bus Stops during the concession period including regular cleaning of the shelter and its surrounding areas, monitoring and functioning of user amenities, handling emergency situations, functioning of information and communication systems, availability of basic infrastructure requirements such as electricity for lighting purposes, proper drainage, removal of municipal solid waste, and telecommunication etc.
- MSI should ensure that the Smart Bus Stop is clean and free of debris, garbage through regular monitoring, maintenance and solid waste collection
- Maintain the Smart Bus Stop and all its components/facilities in good and usable condition and perform routine and periodic maintenance works including civil, electrical & mechanical works as well as maintenance and servicing of furniture & equipment
- MSI should bear all expenses towards the operation of the Smart Bus Stops
- Carry out only those commercial activities at the Smart Bus Stops and clustered amenities or elsewhere that is permitted by ASCDCL, such as advertisements at the Smart Bus Stops and earn revenues from such permitted commercial activities during the concession period
- Transfer Smart Bus Stops and clustered amenities to ASCDCL at the end of the concession period, pursuant to successful completion of necessary inspection, renewals/repairs/replacement
- MSI shall ensure that software and hardware procured for the Smart Bus Stops system is compatible with City Operation Command Centre.
- The integration with the OCC shall be the responsibility of MSI.

MSI shall provide Standard Operating Procedures (SOPs), and user Manuals a step-by-step instruction operate and to resolve the situation quickly and easily.

Smartcity ASCDCL branding at appropriated and aesthetic location

Technical Specifications Applicable as per Annexure
Applicable Government Standards and guidelines must be follow.

Technical solution offer by MSI must complaint to Use cases as per annexure and provision for future addition to use cases

2.7. COMPONENT 7: City Wi-Fi

A. Overview

Proposed locations for City Wi-Fi have been categorized into 3 categories:

- Community aggregation locations – these are locations with audience that are expected to access City Wi-Fi for services mainly for Citizen Services and accessing Government online
- Locations with high footfall – these are locations with audience are expected to access City Wi-Fi for services not limited to Citizen Services and accessing Government online
- Public Bus Stops

The Access Points will be provided at locations as per annexure across the city.

B. Scope of Work

a) The objective is to provide strong, seamless and highly available Wi-Fi for citizens to collaborate and perform business activities on the go. Wi-Fi services will also reduce the digital divide and provide urban dwellers within Aurangabad a better & faster means for connectivity.

b) City Wi-Fi internet access shall be free in select areas in the city, with a maximum download limit of 50 MB per day per user or free for 30 minutes a day whichever is earlier, after which City Wi-Fi services will be available on a paid basis. Offered solution shall allow wireless access through various kinds of devices such as smart phones, laptops, tablets, and desktops. All e- governance applications by AMC, state government and central government shall be excluded from this download limit.

c) City Wi-Fi will be made available to citizens at minimum one (1) mbps speed with a minimum throughput of 100 kbps. Free City Wi-Fi facility should be available as per specified SLAs in the RFP.

d) MSI must ensure that the citizen must be able to use same access details (login id/ username and password) even if he/she moves from one Wi-Fi spot zone to another to provide unified experience of connectivity for the citizen.

e) MSI shall impose restrictions on access and download from malicious sites for City Wi-Fi users. Such sites shall be as notified by TRAI/ regulatory agencies and to be notified to MSI from time to time by ASCDCL.

f) A denied URL list should be applied on this City Wi-Fi SSID and should be updated on a run time basis, to self-learn (no human inference shall be required) and automatically update the list. Any malicious user on the City Wi-Fi should be immediately dropped and blocked after appropriate recording of the evidence.

g) After the free usage of 50 MB per day or 30 minutes of usage, user shall automatically switch over to login page and continue to use by paying as per the data plans else the user will not have the internet access. The rates for paid City Wi-Fi and wired internet services should be competitive to the market rates of the leading data service providers in Maharashtra. MSI must obtain client approval before introducing these rates and any proposed changes in the rates.

h) Hotspots should cover entire area of places given in RFP document. MSI will be responsible for design and engineering of all the network components to meet coverage and capacity requirements of hotspots based on following parameters: Area of Wi-Fi hotspot, Peak load and Density of user devices/ concurrent users/Connections required in the area. Successful Bidder should test the entire location and ensure availability of the Wi-Fi services before declaring it ready for rollout to the client.

i) Based on hotspot capacity requirements, MSI shall determine and provide number of Access points per Hotspot as per the: required Internet bandwidth (both per Hotspot and per user) and aggregated total bandwidth per hotspot. Applicant can consider the contention ratio of 1:10 per user from day 1 of implementation of the project.

j) MSI must assure compliance with All DoT/ TRAI / statutory guidelines/ court orders including all amendments issued from time to time, for the services rendered by them including and not limited to security, including registration of users for accessing the public Wi-Fi.

k) Client (ASCDCL/ AMC) shall not be responsible for any violation of guidelines at any given point of time. MSI is liable for all compliances as required.

l) MSI must ensure appropriate bandwidth allocation for free and paid Wi-Fi users as well for carrying data for all the sub systems with built in scalability for enhanced usage needs as time goes by over the next 10 years. In future if Wi-Fi technology is changed during the contract period to any other technology, the same to be provided by MSI.

m) MSI must ensure the security of the Wi-Fi network and should be able to monitor and manage using appropriate access login controls and audit trails from the Smart City Operations Centre. It should be approved by the client before actual implementation of the same.

n) All Applicants are required to conduct a site survey to address coverage and capacity requirements throughout the areas where hotspots are to be created at their own cost. The coverage maps, where hotspot is to be created, shall be prepared by MSI. It should be approved by the client before actual implementation of the same.

o) MSI must ensure to put up a system in place which can control each registered user's access to Wi-Fi network and the MAC address of the device. Necessary security measures should be enforced along with access control policies and tracking & auditing the usage.

p) All Government advertisement and Government schemes must be published free of cost on the login pages/landing pages. ASCDCL shall take the control of operations in case of any disaster/emergency situations and MSI shall operate under the directions of the appointed ASCDCL.

q) As part of this implementation exercise, the client must get the intelligence about the Wi-Fi service through statistical data, reports and analysis of User registration, Data Usage under various schemes, Network status across the city, device availability, throughput of the internet, Hardware status across the city etc.

r) MSI must provide a web portal for the client to monitor the mentioned indicators and to conduct the necessary audit of implemented system.

s) Client web portal should have a functionality to retrieve various MIS reports. e.g.:

- User wise, Access point wise, connectivity and data usage report in digital format from systems, security events, forensic auditing in given format.
- Other relevant reports as may be required by client, must have to be provided by the MSI
- Blacklisting of users by MAC Address or by checking malicious activity performed by user must be achieved.

Mobile Application and web-based user interface (application to be made available across all leading platforms) should be provided with the following features:

a) Citizen should have an option to enable/ disable connection to city Wi-Fi

b) Registration facility for user to enrol as secured registered user for Wi-Fi

c) OTP based authentication

d) Application should have User Access management module (login, logout functionalities)

e) Application to have feature to track the data consumption for free and paid city Wi-Fi

f) Online/ mobile payment facility for availing paid Wi-Fi service

g) Notification/ alerts to notify user regarding crossing of data usage limit

h) Additional features as required for all intended

i) Separate SSID for free and paid city Wi-Fi for security reasons

j) The administrators should be able to generate MIS report to view overall usage, collections and other usage statistics over a defined time period.

Note: All security guidelines by TRAI/ DoT should be followed for Wi-Fi Security including registration of users on City Wi-Fi.

C. Solution Requirement

Components to be provided and installed by the successful Bidder should perform following functions for throughput and bandwidth requirements

Component	Function
Access Point	Outdoor Wi-Fi Access Point
Industrial Grade Switch – Type 1	Industrial Ethernet Access Switches
WLAN Controller	Wireless Controller to control and manage Wi-Fi Access Points
Network & WLAN Management System	For Network & WLAN infrastructure Management

Key features of Wi-Fi Access points (AP)

a) Network and access points should support creation of robust and reliable mesh network topology based on the field surveys of areas of Aurangabad city (AMC Areas).

b) MSI should perform a detailed survey in AMC area to determine the number of APs required and accordingly configure the number of concurrent users per access point, in a way that there is a fair balance between the hardware costs per AP versus bandwidth cost.

c) Proposed Wired/ wireless and Wi-Fi network architecture should adhere to industry recommended design standards and state of art technology.

d) APs should be installed in outdoor areas and provide last mile connectivity. AP should comply key International and Indian standards for safety, including RF radiations. APs must protect internally stored configuration information.

e) Case-covering must be there for the AP but leaving the antenna out (if external antennas are there) to achieve anti-theft protection.

f) To maintain consistent quality of service for users, network traffic should be prioritized according to applications/users and handled in the AP/Controllers or upstream devices such that the critical traffic is processed immediately, and network congestions are avoided.

Requirements of Wi-Fi Network System

a) MSI has to offer the Wi-Fi management services. Wi-Fi management system should be capable of performing following functions:

- Configuration, enabling-disabling of Access Points as and when required.
- Real-time reporting:
  - Give summary of wireless system status on single management console with graphical user interface which can be customized for future use Inventory of Access Points and their current status.
  - No of APs connected to the network / switches/ repeaters etc. with hierarchy of controls (with IP) as per the design of the Successful Bidder
  - No of users connected to AP with IP of access Points.

Key features of Wi-Fi Controllers

a) WLAN controllers should be, capable of managing at least 1500 Wireless AP and should be scalable as and when required.

b) Controller solution should facilitate monitoring, management, control, and up-gradation from the centralized Smart City Operations Centre.

c) Controllers should communicate back and forth with the centralized security system and network management system in real time.

Key features of Backbone Network

a) Public Wi-Fi network architecture design should include latest BIS, DeitY, IEEE guidelines, and WPC standards for access points

b) Network should support mesh technology and provide seamless and connectivity with the controllers and backhaul network.

c) Backbone Network should perform load balancing users' traffic between multiple access points (umbrella coverage) as well as different bands in an access point so that there is a fair allocation of airtime to each user.

d) Backbone Network should have built-in encryption mechanism to encrypt all communications and data transfer over the Wi-Fi for all the users of Wi-Fi, for sake of security and privacy.

2.8. COMPONENT 8: Outdoor Digital Display and Kiosks

A. Overview

Aurangabad Smart City Development Corporation Limited intends to implement outdoor Digital display and kiosks in the city focused on giving city information to touristsand citizens.

In this era of ultra-connectivity there is a growing demand for cities to become safer, more efficient and more innovative. There is a requirement to transform the urban landscape into hyper connected smarts capes that empower communications to fuel people, neighbourhoods, communities and lives. ASCDCL is committed to working for the benefit of its citizens and tourist with planned implementation of development schemes and is consistently striving to take the city to higher levels of progress. To meet its objective, ASCDCL is aiming to deploy Smart Digital Outdoor full Colour LED Display Panels in ASCDCL area. These information panels will be located at airport, railway station, road side, parks, parking areas, bus stands and other public places, where citizen and tourist foot falls are high.

Purpose of this Digital Outdoor full Colour LED Display Panel is to provide information to citizens and tourists

B. Scope of Work

Design, Development, Implementation, Operation and Maintenance of City Outdoor LED Digital Display System, including:

a. Supply, Installation, Commissioning & Maintenance of Large-size Outdoor LED Digital Display Screens for displaying content/advertisements.

b. Implementation and maintenance of Content Management System to manage the Outdoor LED Digital Display System remotely by providing required connectivity.

c. Content Creation including Information about ASCDCL initiatives and other information provided by ASCDCL and translating it into Videos and Display Advertisements.

d. Engage with advertisers to run the CMS (Content Management System) based advertisements on Outdoor LED Digital Display Screens, for stipulated times as defined, collect revenues, share allocated revenue share with ASCDCL and capture and share time based reports of operations

e. Provide post-implementation on-site support and comprehensive warranty for 5 (five) years for the supplied items.

f. Transfer working Digital Signage Units and CMS system to the city at the end of the contract.

The system will support management of Outdoor LED Digital Display System from a common platform. Allow businesses and others to use their existing web content on multiple form factors, greatly reducing time and cost to deploy new content and applications. Educate the citizens with relevant information in real time, increase visibility of products and services. Increase revenue by providing a platform for third-party advertising. Initially, there will be around 30 such outdoor LED Digital Display Screens. Every such screen will have sufficient bandwidth to support displays.

Scope of work - Kiosk

The City of Aurangabad (the “City”) is seeking proposals from qualified firm(s) for the design, fabrication, installation and operation of interactive digital kiosks (the “kiosks”) in the public right-of-way. The kiosks will be primarily located on sidewalks, and other public areas as approved by the City, and serve the following public purposes, at a minimum:

a. Tourist attraction information – providing information to tourists on various monuments around the city.

b. Way finding – providing information to civic and cultural institutions, transit amenities, restaurants, retail and other business.

c. Transit information – providing information on transit routes and schedule options.

d. Public information and emergency messaging – serving as a central dissemination point for information.

e. Increased vibrancy and visual interest of City streets – promoting placemaking in Aurangabad through City events and programming.

f. Enhance tourism experience of Aurangabad – advancing Aurangabad’s narrative to Tourists.

g. Accessibility, usability and inclusion – creating a welcoming and inclusive technology for our tourist community at large

h. Act as the backbone to the City’s public-facing, smart city infrastructure, which would allow other technologies to be deployed (e.g. community connectivity through public Wi-Fi and environmental sensors).

i. Multi language Support like Marathi, Hindi and English

Planning and Installation

System Planning and approvals from the client the client or the Bidder will propose a list of locations.

The Bidder is required to review these locations and give their recommendations on the same which shall be taken by the client for consideration.

The Bidder may also propose multiple locations for the Kiosk as per the need of the business.

Installation Schedule

The number of Kiosk at the time of formal launch shall be as decided by the client.

Technical Standards

All the Kiosk shall be of at least with the specifications as mentioned in the Annexure . The Bidder will ensure that all Kiosk procured for the project are new and have not been put to commercial use anywhere prior to the Commencement of Operations. The Bidder will present prototype Kiosk for the Smart Kiosk System to client for inspection. Client will have the right to review all hardware and software to ensure they meet all the technical criteria as specified. Client will accept a prototype, which may have features over and above the prescribed minimum standards. Should client find any discrepancy between the prototype and the technical specifications, the bidder will have 30 days to propose a solution. The final designs will be subject to approval from the client. After receiving approval on the final design, the bidder may proceed to manufacture/ acquire the rest of the Kiosk. The bidder shall provide aesthetically good colours and design on the Kiosk and a logo of the client (AUTHORITY) should be a part of the design and should be clearly visible on the Kiosk and at the major Smart Kiosk areas.

Kiosk Design

The City is flexible in regards to the proposed Kiosk design. Proposed solution should include a detailed representation of Kiosk Design Plan, including multiple graphic renderings of the Kiosk Design, including renderings of the proposed design(s) on the right of way. Companies are encouraged to submit multiple designs for consideration by the City.

Human Resource Plan

The Bidder will

i. Enlist trained professionals to operate the Kiosk System

ii. Hire adequate staff to ensure that scope of services as mentioned in the RFP are met

Number of Kiosk- Size

i. Procure Kiosk as per the requirements of the client, each of which shall comply with the technical standards. The size of the Kiosk can be increased at the discretion of the client.

ii. Procure and maintain Standby Kiosk as may be determined by client to ensure that the operational size remains above or at the stipulated size level.

In general, the incremental change in size can be made by client and the Concessionaire on an ad-hoc basis depending on the need/ demand.

The Service Levels are required to be complied with by the Concessionaire as per the service level benchmarks of this document. Failure to comply with these service levels will attract penalties as specified.

Hours of Operation

As per working hours (and in some cases 24 X 7) of the location. The client shall provide space and suggest locations for of Kiosk. The same shall be decided based on the decision and approval of the concerned departments of the city. The same will be increased / changed / decreased as per requirement.

Data Transfer to client

All transactions (cash/ card) shall be registered electronically on the system. The monthly MIS shall be submitted to the client.

User Information System

It is required that a Call Centre be set up to provide user support during all hours.

Data Reporting

During the Operation Period,

The Bidder shall make available all the data pertaining to the Operation & Maintenance of the Project real-time that can be accessed by the client or its representative. The real-time data shall be in such a format that the client shall be able to evaluate the performance of the Concessionaire against the Service Levels set forth in this Agreement.

The client may request the Bidder for any additional information other than the real-time data if need be.

Advertisement Space

All rights to advertising, sponsorship, naming, and branding rights associated with the system will remain with the Client . Advertisement(s) should be non-political and should be authorized by the client before implementation. Client logo and material may be required to be put in any advertising or marketing material related to this contract

C. Solution Requirement

The project can be divided into two major parts: (a) Design, Development, Implementation, Operation and Maintenance of City Outdoor LED Digital Display System, and (b) Content Creation, Content & Advertisement Management. It is proposed to install Outdoor LED Digital Display System in ASCDCL area. These Outdoor LED Digital Display Screens will be installed in phases.

a) **Outdoor LED Digital Display Screens:** Outdoor LED Digital Display Screens should have following provisions:

- Panel should have 1920 x 1080 Resolution (Full HD) or better.
- Managed remotely by an advanced, web-based management portal and content management software.
- LED screens enclosure should be in a protective shell made of robust weatherproof material, it would be placed outdoor, such that it should survive adverse weather conditions. ASCDCL logo/ASCDCL messages shall be pasted on each enclosure below LED screen as per ASCDCL directions. The LED screens shall be centrally managed and there shall have enough provision for bandwidth to support all remote locations.
- It shall be a comprehensive solution featuring Outdoor LED Digital Display System, Screens and ASCDCL information.
- Designs of Outdoor LED Digital Display Screens must achieve aesthetic excellence and must be compatible with a wide variety of built contexts. Designs will be evaluated on the basis of functional efficiency, aesthetics, security, durability, adaptability for various built environments around Aurangabad, including historic places and individual landmarks, and accommodation of people with disabilities. All designs are subject to the approval of the ASCDCL.
- MSI has to submit at least two basic designs of Outdoor LED Digital Display Screens. The design shall be suitable for deployment in Aurangabad area. All components of the Outdoor LED Digital Display Screens must be fabricated of high quality, durable, maintainable and vandal-resistant materials. To the maximum extent feasible, all surfaces of the Outdoor LED Digital Display Screens that are accessible to the public must be graffiti-resistant. Footings shall be imbedded in the sidewalk so that there are no surface plates to create a trip hazard.

b) Solution Design

ASCDCL Outdoor LED Digital Display System should bring together displays, web technologies, multimedia, and collaboration into an integrated solution. The solution should allow businesses and public agencies to combine applications built on web technologies for consumer, passenger, and citizen information as well as marketing and Smartcity ASCDCL branding promotions.

Solution should consist of computing and collaboration devices, management platform, and a network infrastructure to deliver web-based applications and multimedia content through displays and through Outdoor LED Digital Display Screens to end users in ASCDCL areas.

Central management console will be used to remotely configure, control, and monitor Outdoor LED Digital Display System. Central manager should provide user management as well as real-time monitoring, live viewing of remote screen content, notification of events, and session management.

Outdoor LED Digital Display System computing devices should support registration in the central manager either individually or in batches. Central Manager should be accessible through a web portal with a menu-based program. Central Manager should support Accounts creation to segregate users, devices, and policies. Users should be assigned to a particular account. They can then configure and manage the devices associated with that account. Manager should monitor Outdoor LED Digital Display System and its devices at regular intervals. The status of the devices should be collected within a period of time set by the user. Users should be notified when the status of devices in their account changes.

Device logs should be sorted and analysed by clicking the Events tab of a device. Similarly, the device’s performance should be monitored by viewing the Performance report of a device. The software should be capable to send logs to a third-party server.

A policy is a restrictive mechanism, providing the user with a tool to enforce certain behaviour. Policies represent dynamic and transportable setup rules. Policies can be persistent (long-term) or transient (short-term) and can be scheduled per Outdoor LED Digital Display System based on time or events.

c) Solution Capabilities

- Should support management of Outdoor LED Digital Display System from a common platform. Allows businesses and agencies to quickly use their existing web content on multiple form factors, greatly reducing the time and cost to deploy new content and applications.
- Enable new services to improve customer experiences and increase customer retention with consistent end-user experiences across multiple endpoints.
- Educate the customer with relevant information in real time, increase visibility into products and services offered, and increase revenues by providing a venue for third-party advertising.
- Reduce costs with increased operational efficiency in customer and business processes, increase operational consistency by enabling reuse of existing web content, simplify deployment, and reduce use of management resources with remote manageability.
- Reduce deployment and management timelines using policies and groups.
- Improve management experience with integrated solution architecture.
- Above topology shows high level solution requirement where MSI should plan and implement overall network which includes both data centre and Outdoor LED Digital Display System connectivity.
- Every such screen should have minimum bandwidth to support displays. MSI should also define data centre side bandwidth requirement based on total number of Outdoor LED Digital Display Screens. MSI will also pay for electricity requirements to operate the display panels. ASCDCL shall ensure provision of electrical connection to the Outdoor LED Digital Display Screens.
- MSI should manage the content management based on ASCDCL requirement. MSI should plan data centre requirements and also include all necessary items required for hosting the system. MSI should also provide and manage all necessary equipment required for Outdoor LED Digital Display System to operate.

Content Creation: Content creation will include but not be limited to the following. ASCDCL retains the right to increase the content by 30% during the period of the contract.

- City Videos, 6 in total, 2min to 5min each
- City Overall Tourism Video
- Ajanta Ellora Video
- Foods Trail Video

- Art & Crafts Trail Video
- City Citizen Initiatives Video
- City Economic Pivot Video
- City Image based Collaterals
- Link information from city systems, initiatives, happenings, weather etc.

Digital Films/City Videos: Short promotional digital films can be extremely effectual for raising awareness, informing and educating the citizens about various activities/schemes/procedures. Key messages from ASCDCL and Aurangabad Tourism Vision must be taken and content in terms of print/audio/videos/images must be made by the MSI. It should be a form of Digital storytelling with Aurangabad as a backdrop. These videos could be related to tourism, economy, citizens, health, sanitation, water usage, or various key messages to be conveyed from other departments of ASCDCL. MSI will be responsible for conceptualizing, creating and producing the films under this engagement. All videos shall be freshly shot for this engagement. All graphics/animations/images to be used should be developed or bought under applicable laws for the end consumption for ASCDCL.

MSI will be responsible for conceptualizing and developing content in different formats like text, info graphics, dashboards, jingles, short films/documentaries, training films, audio visual material in any other formats as per requirement.

MSI will also help the conceptualization and design material for Outdoor LED Digital Display Screens. MSI shall ensure that all audio, video, image and information content should follow guidelines laid down by Ministry of Information and Broadcasting (I&B) and Directorate of Advertising and Visual Publicity (DAVP).

MSI shall ensure the authenticity of materials used for content creation, including legal sourcing of real footage and images; credible sources for information; video content vetted by ASCDCL appointed media expert.

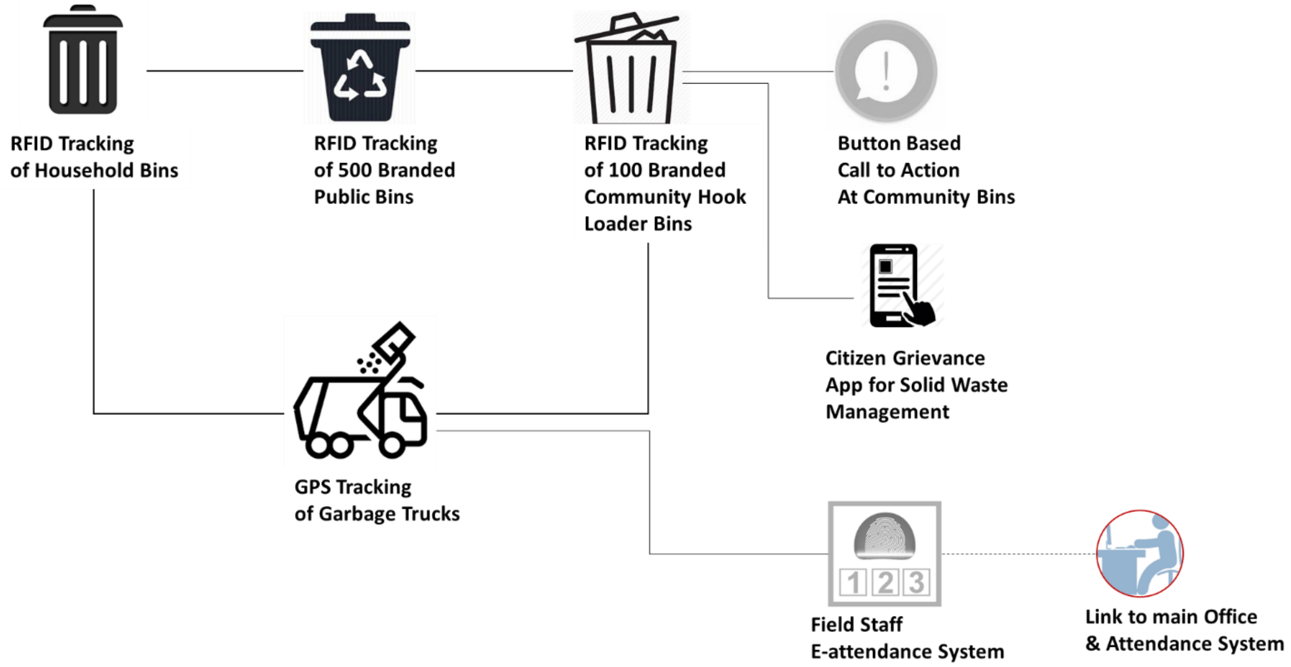
2.9. COMPONENT 9: ICT Enabled Solid Waste Management

A. Overview

For the betterment of citizens Aurangabad Municipal Corporation has taken initiative under the smart city mission and the aim is related to Solid Waste Management under Swachh Bharat Mission and development of open and green spaces. To provide better facilities and services for citizens of Aurangabad Municipal Corporation, AMC is using new technology for the smart city mission. The main purpose of this initiative is to manage the movement of solid waste pick up, movement of water tanker and other vehicle through various technologies like GPS Tracking System, UHF RFID Reader along with innovative Mobile and Web based application to improve and smoothen ground level mechanism for waste collection, disposal and distribution of water through water tankers and attendance of the ground staff

Challenges Faced at Present for all fleets:

- Difficulty in tracking of vehicles and their movement
- No proper mechanism for calculating their total trips, distance travelled per day
- Difficulty in ensuring that the vehicle attends the routes / societies at the specified time or whether the garbage has been collected.
- Difficulty in performance measurement, measuring trip counts and contractor payment calculation
- Difficult in addressing citizen complaints
- Difficulty in ensuring actual and timely pickup of bins
- Difficulty in identification of bins.
- Difficulty in determining the fill level of bin.
- Difficulty in preparing payment report of contractors as it’s manual processes.
- No proper reporting system of number of vehicles inside Dump Yard at particular moment.
- No proper mechanism for calculation weight and send it to existing GPS Software
- No proper mechanism of attendance for Swachh workers, NGO and municipal staff.
- No proper mechanism to calculate the number of trips and water dispensed per water tanker


RFID Tracking of Household Bins
RFID Tracking of 500 Branded Public Bins
RFID Tracking of 100 Branded Community Hook Loader Bins
Button Based Call to Action At Community Bins
Citizen Grievance App for Solid Waste Management
GPS Tracking of Garbage Trucks
1 2 3
Field Staff E-attendance System
Link to main Office & Attendance System

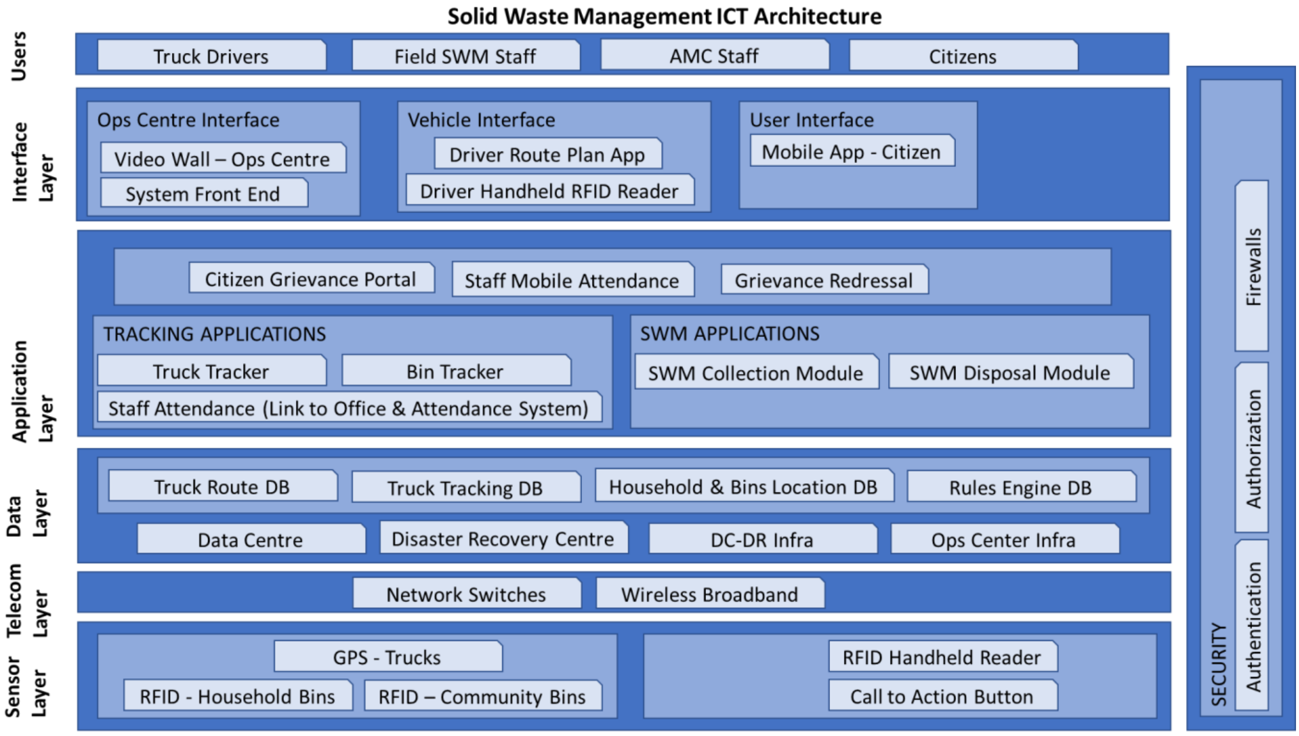
B. Scope of Work

To integrate the Vehicle Tracking System on AMC Vehicles and to provide a modules and reports for garbage weight calculation automatically in the software, Trip counts for each type of vehicle based on their nature of work, Contractor payment and penalties calculation automated, Unauthorized vehicle movement and exception reports based on defined SLAs for drivers and contractors, Paperless system and no manual intervention for all bills and reports calculation.

The solution will be monitored centrally from existing Control Centre Below are primary objectives of the Solid Waste Management (SWM) monitoring & tracking solution

- Provide real time tracking of vehicles.
- Control room for monitoring - Fleet Analyst
- Dashboard and Summary of Vehicles (Each Fleet)
- Alert – over speed, excess stoppage time, excess fuel withdrawn
- Fleet Daily & summary Report
- Idle Time /Journey Idling Report
- Start time & End time, Total working hours, Distance travelled
- Stoppage & Speed Violation
- History playback/ Route replay
- Maps
- Automate the transfer stations and disposal site for daily garbage inward and outward activities

- To utilise the technology to minimize human intervention and to improve the collection efficiency
- To full proof the system and prevent misuse of manual system and to induct transparency and accountability in operations
- To monitor the attendance of the employees and workers involved
- To have the system that helps monitor the performance and SLA for Contractors with Penalties
- To supply, install, configure, commission and maintain the RFID readers and RFID Tags in SWM vehicles and Container Bins.
- To supply volume sensors to monitor the fill level of the bins.
- To supply, install, configure and maintain the Biometric Device for taking attendance of the employees and Swachh workers.
- To design, develop, configure and maintain the SWM application for carrying out business processes at Primary Transfer Station, Disposal Site, Solid Waste Management Department, Zone & Ward to monitor and manage the Solid Waste Management activities.
- To supply, install, configure and maintain the application server to be placed at AMC data centre.
- Provisioning of customizable reports required for day to day and periodic monitoring and MIS purpose.
- Facility to generate alerts for specific events on the screen and also by SMS.
- To make available the data as per the formats and as per time intervals given by corporation
- Facility to create new entity / contractor with contract details (contract start date, end date, zone, wards, etc.)
- Defining of payment terms, SLA, etc.
- Map vehicles to contractors
- Map drivers to contractors
- Application code and executables along with platform specifications for GPS /AVL Engine shall be submitted with the solution



I. Payment and Penalty Calculation Module

The payment to the contractor is based on the no. of trips. The contractor is required to provide the services as per the SLAs defined. The payment and penalty calculation should be possible through this system. The contractors are awarded payment based on certain condition. Also, penalties are calculated based on certain conditions. The solution should have business rule configuration module where penalty conditions can be configured. These business rules should be taken into consideration while calculating final payment amount to be paid to the contractor. This module should enable to generate payment reports capturing performance of the contractor depending on various performance SLAs and KPIs like missed POI, tonnage collected, etc.

For e.g. for the Door to Door Garbage Collection penalties are levied if the vehicles do not start and end the collection activity in time, if the vehicle misses any society/building (missed POI), etc

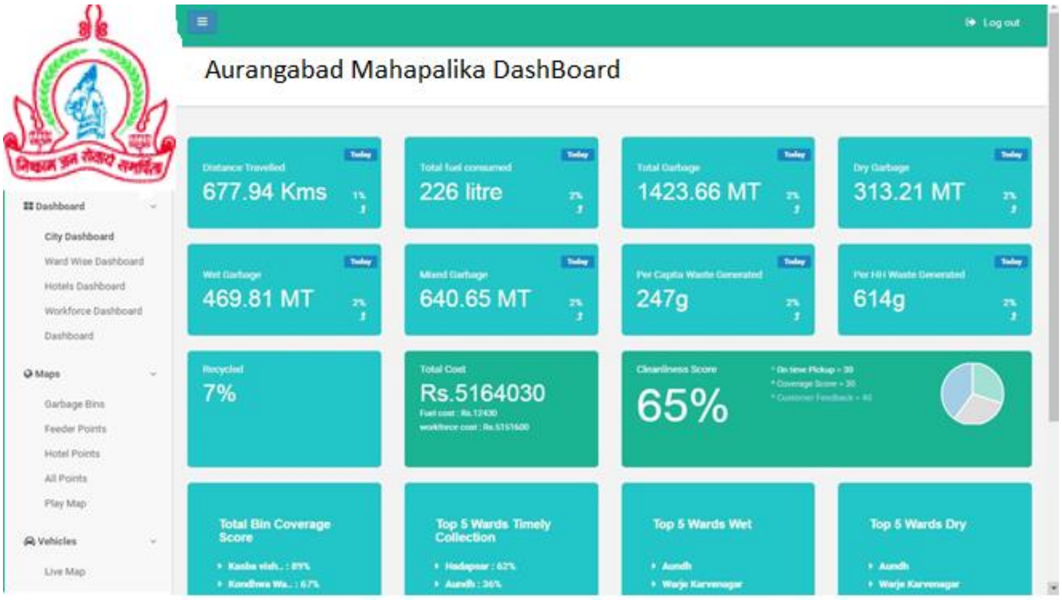
II. MIS Reports

1. Verification Report & Exception reports to be developed
2. Date wise, Zone wise list of vehicles transferred / not transferred garbage to Transfer Station.
3. Vehicle wise, date wise vehicle in operation / not in operation details.
4. Date wise, vehicle wise number of trips at disposal site.

5. Date wise list of abnormal vehicles whose number of entries into dump yard not matches.
6. List of vehicles present into dump yard at any moment.
7. Date wise, Zone wise list of vehicles with non-functional GPS.
8. Payment report for Contractors (Based on weight/trips per vehicle per day)
9. Penalty report for Contractors (Based on weight/trips per vehicle per day)
10. Not moving vehicle Report
11. Not Reporting Vehicle Report
12. Less than 5km Travelled Vehicle Report
13. Over Speeding Vehicle Report

Following are few Indicative reports.

Dashboard



Aurangabad Mahapalika DashBoard

Distance Travelled — Today — 677.94 Kms — 1%

Total fuel consumed — Today — 226 litre — 2%

Total Garbage — Today — 1423.66 MT — 2%

Dry Garbage — Today — 313.21 MT — 2%

Wet Garbage — Today — 469.81 MT — 2%

Mixed Garbage — Today — 640.65 MT — 2%

Per Capita Waste Generated — Today — 247g — 2%

Per HH Waste Generated — Today — 614g — 2%

Recycled — 7%

Total Cost — Rs.5164030
Fuel cost : Rs.12430
workforce cost : Rs.5151600

Cleanliness Score — 65%
* On time Pickup = 30
* Coverage Score = 30
* Customer Feedback = 40

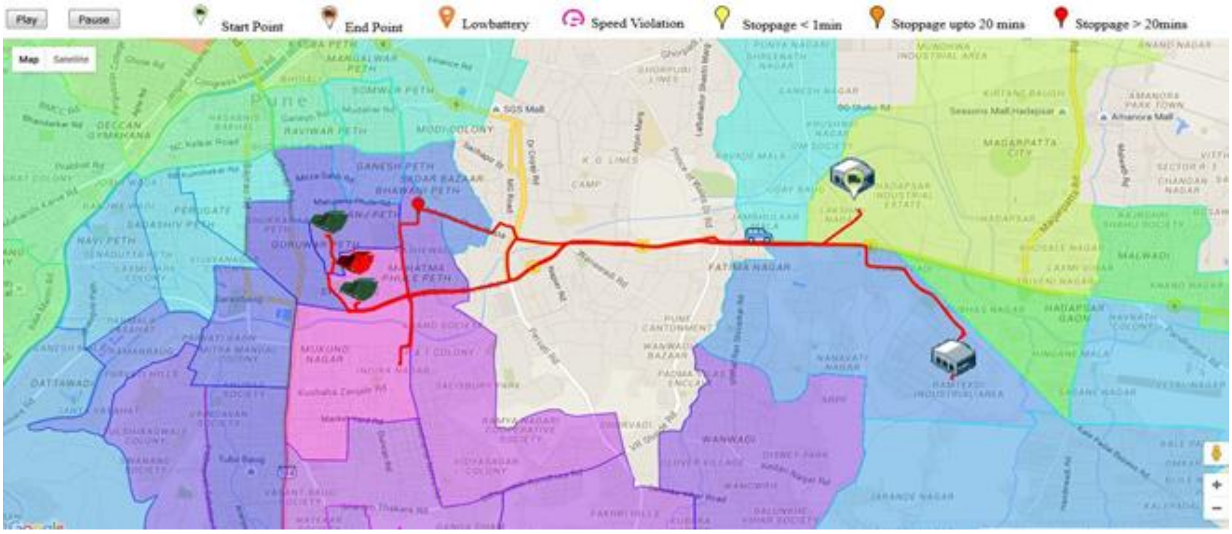
Total Bin Coverage Score
- Kasba vish.. : 89%
- Kondhwa Wa.. : 67%

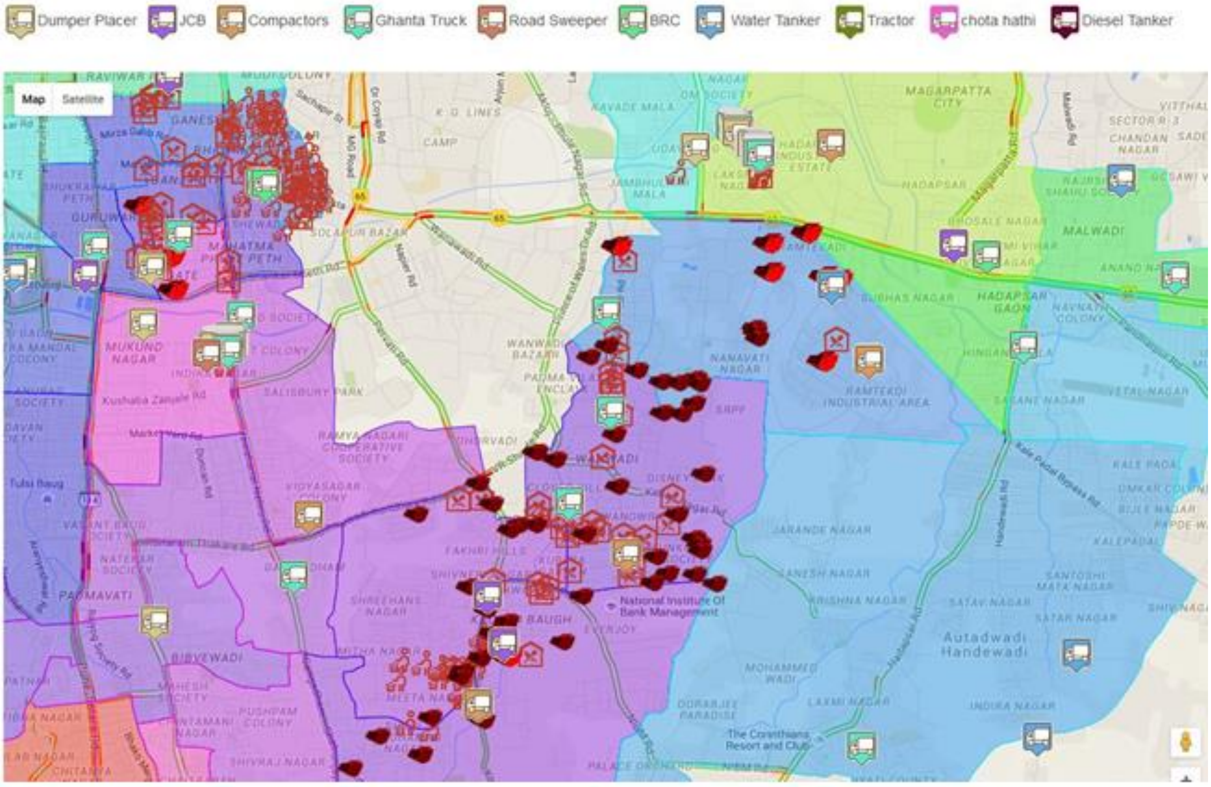
Top 5 Wards Timely Collection
- Hadapsar : 62%
- Aundh : 36%

Top 5 Wards Wet
- Aundh
- Warje Karvenagar

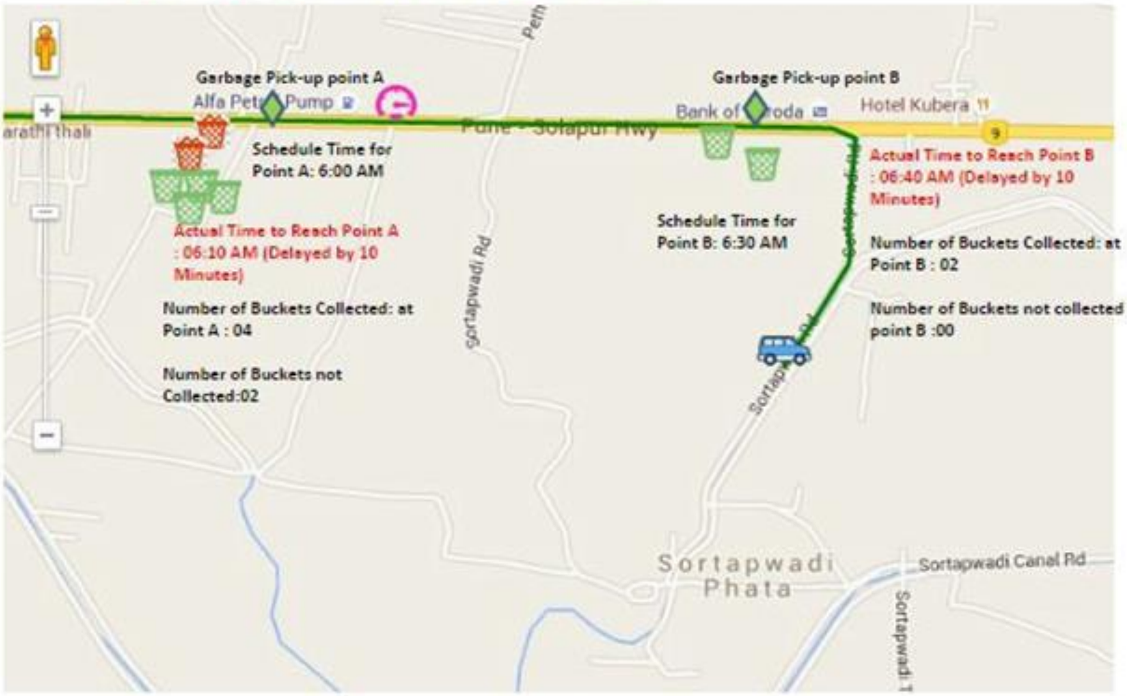
Top 5 Wards Dry
- Aundh
- Warje Karvenagar

Single view Dashboard





MAP VIEW for the Vehicle Work Status


Peth
Garbage Pick-up point A
Alfa Petrol Pump
arathi thali
Schedule Time for Point A: 6:00 AM
Actual Time to Reach Point A : 06:10 AM (Delayed by 10 Minutes)
Number of Buckets Collected: at Point A : 04
Number of Buckets not Collected:02
Pune - Solapur Hwy
Sortapwadi Rd
Garbage Pick-up point B
Bank of Baroda
Hotel Kubera
Schedule Time for Point B: 6:30 AM
Actual Time to Reach Point B : 06:40 AM (Delayed by 10 Minutes)
Number of Buckets Collected: at Point B : 02
Number of Buckets not collected at point B :00
Sortapwadi Phata
Sortapwadi Canal Rd

The above Map View Shows that the Vehicle was schedule to reach Point A at 6:00 AM but actually reached at 6:10 AM (Delay by 10 minutes) and collected Total: 6 Garbage Buckets from Point-A & Point-B

III. Requirement of Hardware at Transfer Station and Disposal Site

- RFID Readers: - The RFID reader should be installed at transfer stations, processing plant, ramps and disposal site. These readers would fetch vehicle details automatically from RFID tags placed on each vehicle in such a way that supervisor would not have to enter vehicle details manually.
- Boom Barriers: - The Boom Barrier should be installed at transfer stations, processing plant, ramps and disposal site. This will strict the unauthorized vehicle entry and only allowed vehicles will enter
- Cameras: - The cameras should be placed at each transfer station and disposal site to monitor entry and exit of vehicles. The cameras would be used to capture image of vehicle (with number plate visible) directly in the system at the time of saving record. (ANPR Camera + 4 Port POE Switch + 4 Channel NVR + iVMS Software)
- Biometric devices: - Mukadam/Supervisor will use handheld biometric attendance device to mark the attendance of the Swachh employees/truck drivers/remote workers/field staff at various locations
- RFID tag to be installed on vehicle (Refused Compactor and Dumper Placer)
- The solution should have capability to integrate with Email and SMS gateway to send Email and SMS. AMC will provide email and SMS gateway with necessary api.

SMS and Email gateway integration will be the responsibility of bidder.

- The solution should be accessible from smart devices (e.g. iOS/android cell phones, tablets etc.)
- The bidder will be required to implement necessary data archival policy for the solution. Bidder to archive historical data as defined by AMC and to make available the archived data in usable format on requirement of AMC.
- Internal & External Integrations: The required application should be developed with latest technologies and should be open with integrations with other applications/portals of the Department. The captured data may be required to be integrated with various internal & external interfaces.
- The solution should be scalable and should not have any restrictions on number of users using the solution, licenses, number of vehicles getting tracked and hardware devices integrated.

IV. SLA for contractor

1. **Tractor Vehicle / Ghanta Gadi:** In case of tractor / tipper vehicle the payment is made on the basis of trip count i.e visit to the transfer station. But they are expected to carry a specified weight. Concerning the same the following is expected
    a. Payment will be made depending on the number of trips
    b. Trips to be only considered if the weight bought exceeds or equals the expected weight.
    c. If weight is less than the expected weigh the approval for trip to be considered genuine should be in the hand of the supervisor or concerned authority.
2. **Water Tanker:** In case of water tanker the payment is made on the basis of trips i.e collection of water from filling station and delivery at requisite location. But the same cannot be uncertain. Concerning the same the following should be implemented
    a. Geo fencing for the vehicle route should be done to ascertain the concerned deliver and monitoring of route.
    b. Payment to be also done by taking in account customer acceptance receipt.
3. **Road Sweeper:** Road sweeper is used for sweeping off roads and the payment is done on the basis of Kilometre covered. But there is no mechanism for ensuring if the roads are swept and the schedules are meet. For the same following should be undertaken.

   a. Along with the Kilometre running the Schedule punctuality should be also kept in mind. for making payment

   b. Any missed schedule should be reported and the contractor is supposed to justify for the same to the authority or the administration.

4. **JCB:** These vehicles are used for construction and road works. Payment are made on hourly basis, but there is no way to determine how much of the vehicle services was used during that time. Concerning the same the following should be considered

   a. Instead of the hourly payment system, the payment should be on the basis of the engine running time / switched on time.

5. **BRC:** These vehicles are used for transferring garbage from transfer station to disposal site and the payment for the same is made on the trips undertake. But there is no mechanism to uncertain the schedule management and the tonnage of garbage being carried. Concerning the same the following should be considered

   a. The driver should adhere to the time scheduling and any delay in the same should be reported to the supervisor or the administrator.

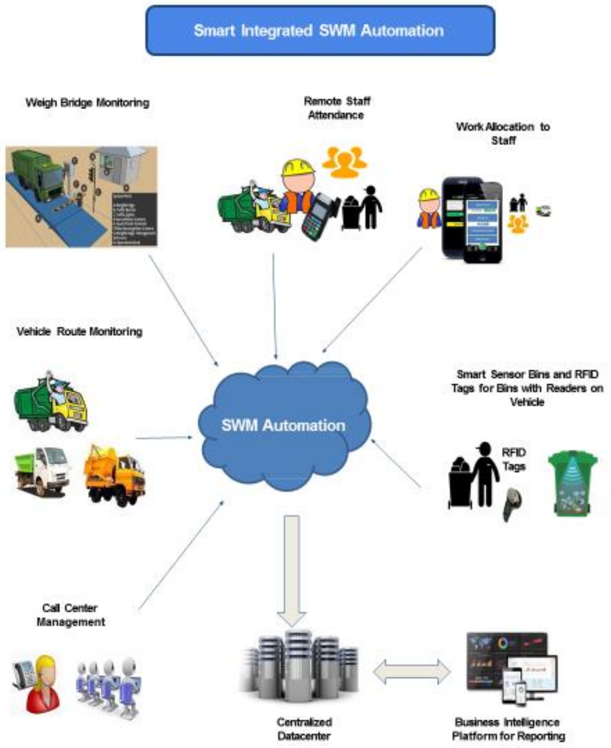
   b. The tonnage of garbage should be monitored while leaving transfer station and while entering the disposal site so as to ensure the quantity of garbage is same and it’s not disposed somewhere else apart from the allocated site.

V. GPS Analyst for GPS System Monitoring and Reporting

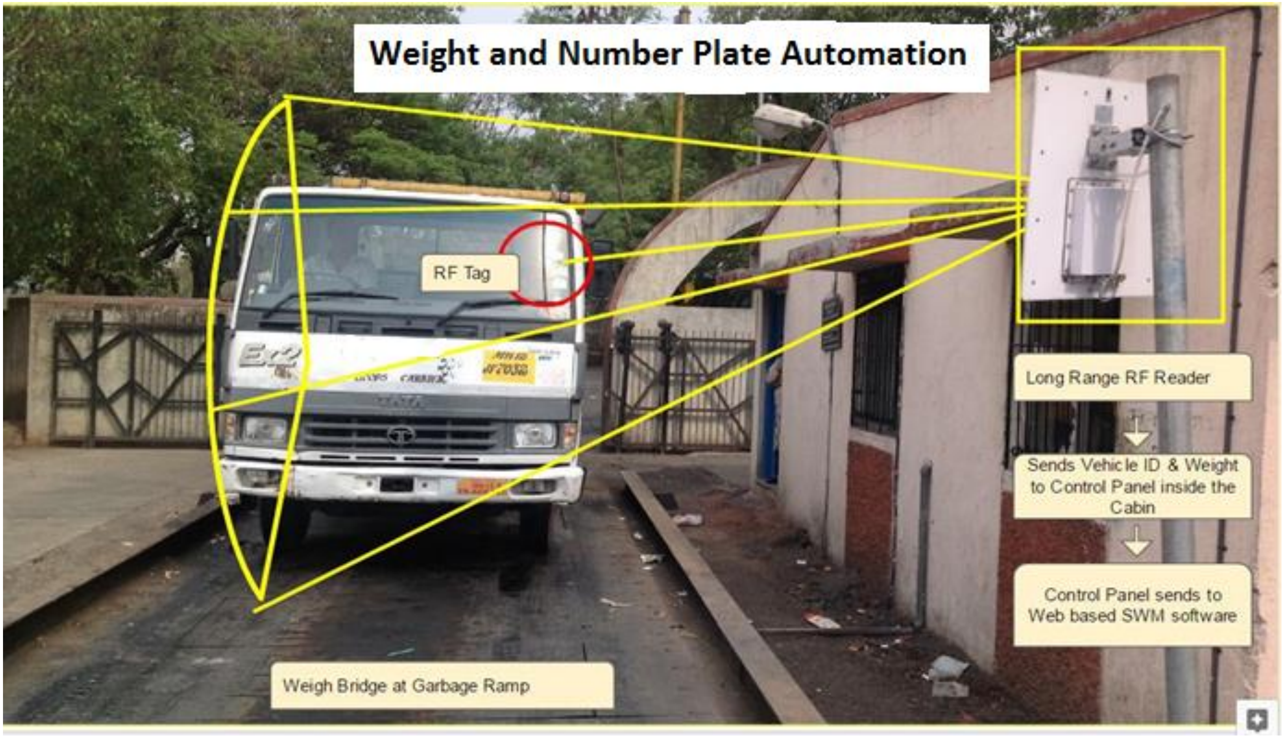
GPS Analyst will be required for Coordination with Municipal Corporation Persons for handling the technical aspects and the issues related to GPS tracking on Garbage Collection Vehicles. They will monitor the system and will communicate and coordinate with ward level for relevance of the issue Also will report the violations if done by any Garbage Collection Vehicle and at the end of the day he will submit the desired report like pickup of particular bin done by vehicle or not with violation report on daily basis.

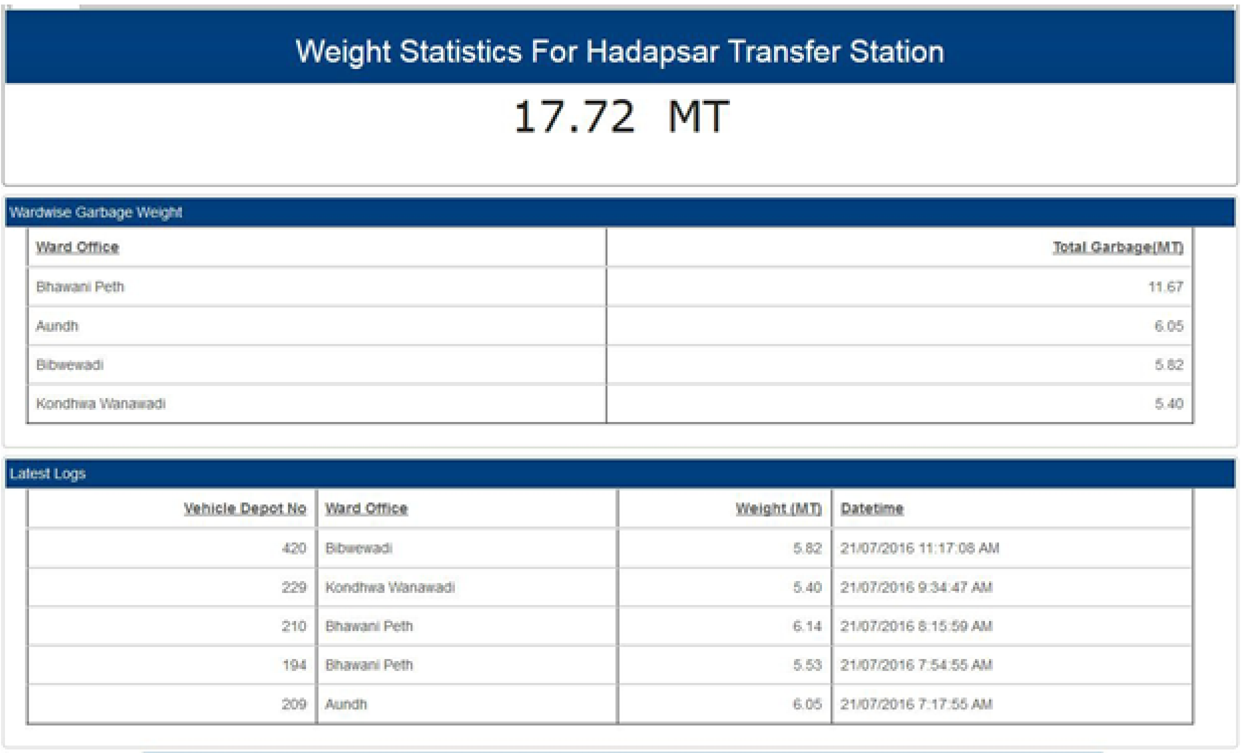
C. Solution Requirement

AMC invites the bids to have the Smart Solid Waste Management System that helps overcome the challenges mentioned above. The Smart Solid Waste Management Solution will broadly comprise of the following:



- GPS Device on all vehicles
- RFID tags on waste collection vehicles
- RFID readers at transfer stations and disposal site
- Cameras to capture image of vehicle (along with number plate) entering and exiting transfer station and disposal site
- Integration with weighing scale to capture weight data of loaded and empty vehicles.
- Biometric system to take attendance of Swachh workers, NGOs and ground staff


Weight and Number Plate Automation
RF Tag
Long Range RF Reader
Sends Vehicle ID & Weight to Control Panel inside the Cabin
Control Panel sends to Web based SWM software
Weigh Bridge at Garbage Ramp



Weight Statistics For Hadapsar Transfer Station

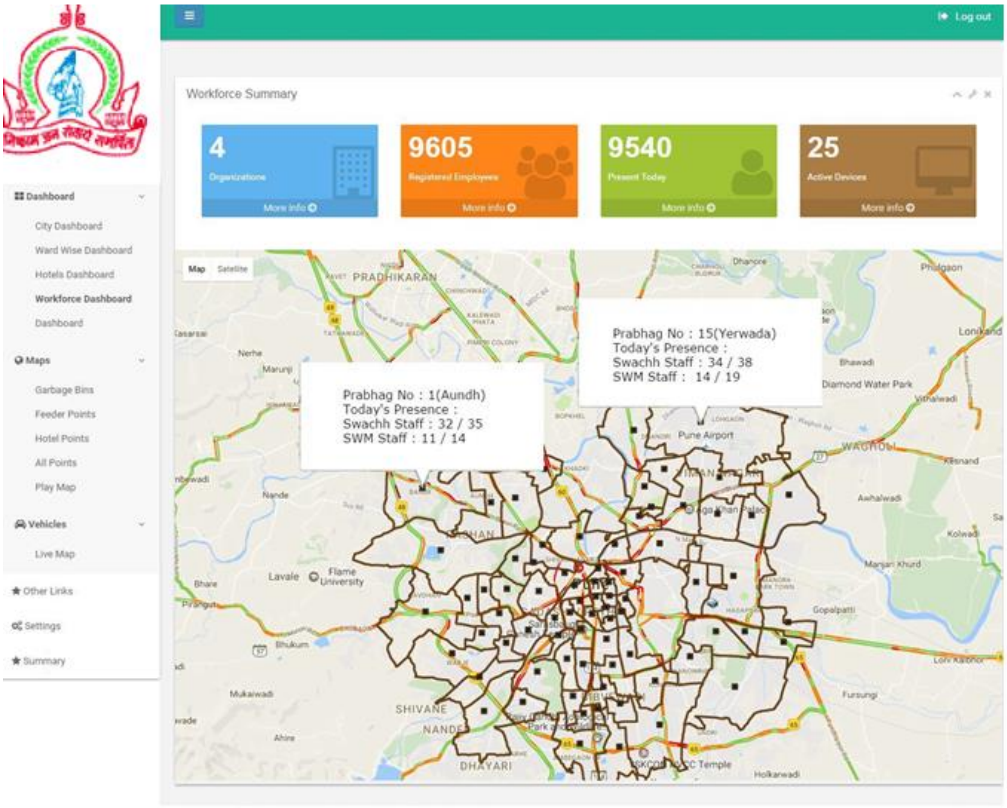
17.72 MT

Wardwise Garbage Weight

Ward Office	Total Garbage(MT)
Bhawani Peth	11.67
Aundh	6.05
Bibwewadi	5.82
Kondhwa Wanawadi	5.40

Latest Logs

Vehicle Depot No	Ward Office	Weight (MT)	Datetime
420	Bibwewadi	5.82	21/07/2016 11:17:08 AM
229	Kondhwa Wanawadi	5.40	21/07/2016 9:34:47 AM
210	Bhawani Peth	6.14	21/07/2016 8:15:59 AM
194	Bhawani Peth	5.53	21/07/2016 7:54:55 AM
209	Aundh	6.05	21/07/2016 7:17:55 AM



Log out

Dashboard
- City Dashboard
- Ward Wise Dashboard
- Hotels Dashboard
- Workforce Dashboard
- Dashboard

Maps
- Garbage Bins
- Feeder Points
- Hotel Points
- All Points
- Play Map

Vehicles
- Live Map

Other Links

Settings

Summary

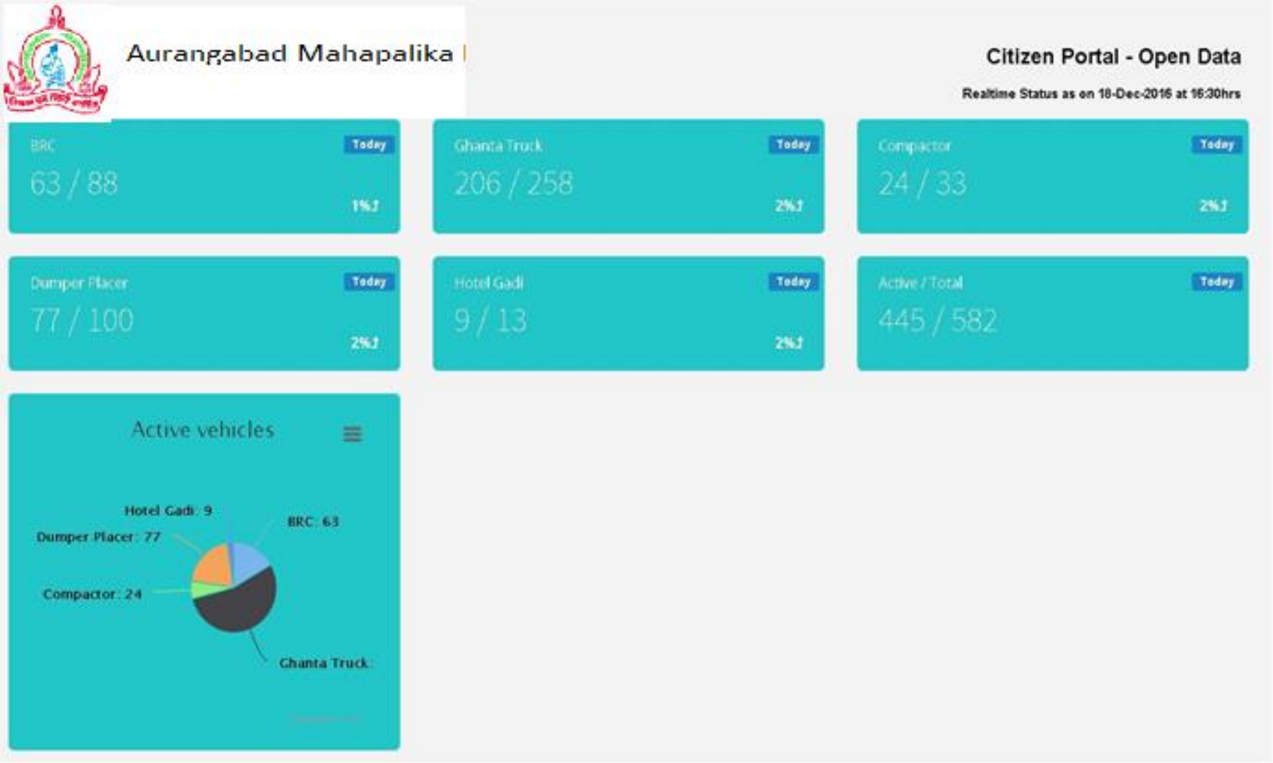
Workforce Summary

4	9605	9540	25
Organizations	Registered Employees	Present Today	Active Devices
More info	More info	More info	More info

Map Satellite

Prabhag No : 1(Aundh)
Today's Presence :
Swachh Staff : 32 / 35
SWM Staff : 11 / 14

Prabhag No : 15(Yerwada)
Today's Presence :
Swachh Staff : 34 / 38
SWM Staff : 14 / 19



Aurangabad Mahapalika

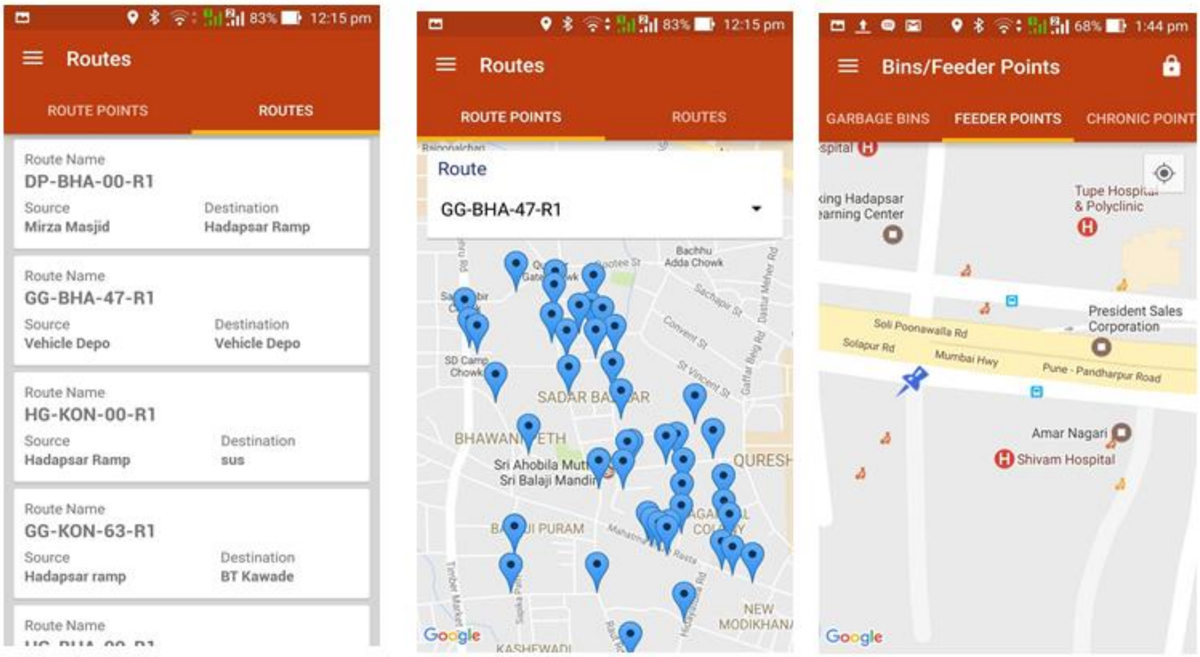
Citizen Portal - Open Data

Realtime Status as on 18-Dec-2016 at 16:30hrs

BRC	Ghanta Truck	Compactor
Today	Today	Today
63 / 88	206 / 258	24 / 33
1%	2%	2%

Dumper Placer	Hotel Gadi	Active / Total
Today	Today	Today
77 / 100	9 / 13	445 / 582
2%	2%	

Active vehicles



83% 12:15 pm

Routes

ROUTE POINTS ROUTES

Route Name	
DP-BHA-00-R1	
Source	Destination
Mirza Masjid	Hadapsar Ramp

Route Name	
GG-BHA-47-R1	
Source	Destination
Vehicle Depo	Vehicle Depo

Route Name	
HG-KON-00-R1	
Source	Destination
Hadapsar Ramp	sus

Route Name	
GG-KON-63-R1	
Source	Destination
Hadapsar ramp	BT Kawade

Route Name

83% 12:15 pm

Routes

ROUTE POINTS ROUTES

Route

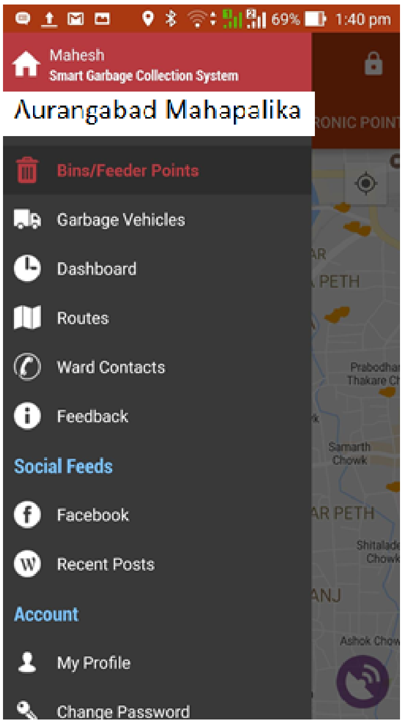
GG-BHA-47-R1

68% 1:44 pm

Bins/Feeder Points

GARBAGE BINS FEEDER POINTS CHRONIC POINT

Citizen App Indicative Screens



69% 1:40 pm

Mahesh
Smart Garbage Collection System

Aurangabad Mahapalika

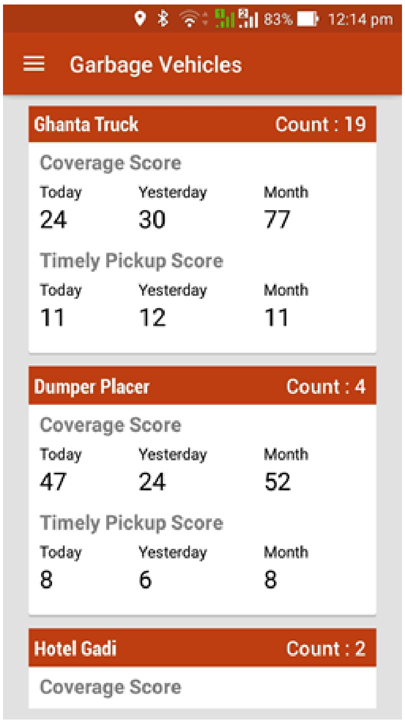
- Bins/Feeder Points
- Garbage Vehicles
- Dashboard
- Routes
- Ward Contacts
- Feedback

Social Feeds

- Facebook
- Recent Posts

Account

- My Profile
- Change Password



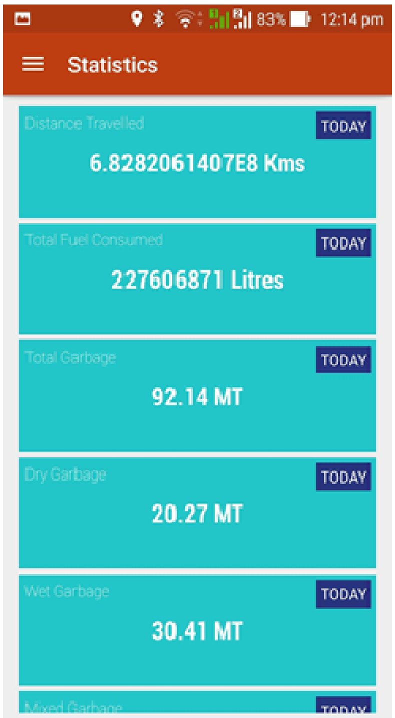
83% 12:14 pm

Garbage Vehicles

Ghanta Truck		Count : 19
Coverage Score		
Today	Yesterday	Month
24	30	77
Timely Pickup Score		
Today	Yesterday	Month
11	12	11

Dumper Placer		Count : 4
Coverage Score		
Today	Yesterday	Month
47	24	52
Timely Pickup Score		
Today	Yesterday	Month
8	6	8

Hotel Gadi		Count : 2
Coverage Score		

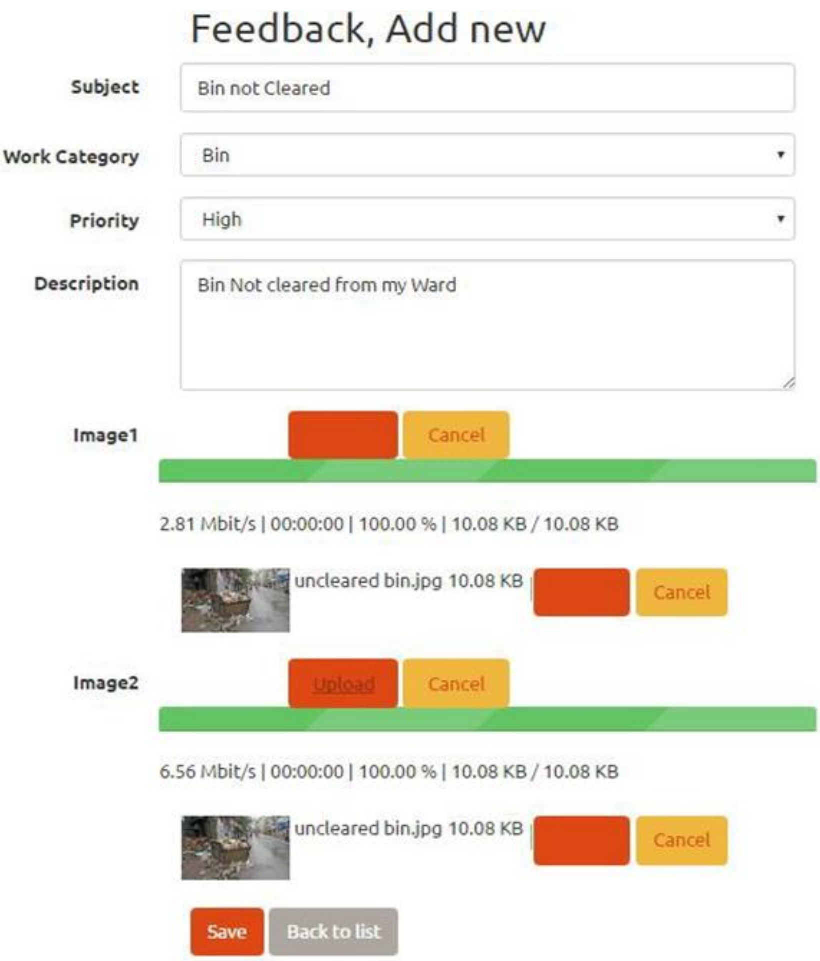


83% 12:14 pm

Statistics

Distance Travelled	TODAY
6.8282061407E8 Kms	
Total Fuel Consumed	TODAY
227606871 Litres	
Total Garbage	TODAY
92.14 MT	
Dry Garbage	TODAY
20.27 MT	
Wet Garbage	TODAY
30.41 MT	
Mixed Garbage	TODAY

Feedback form Indicative Screen



Feedback, Add new

Subject: Bin not Cleared

Work Category: Bin

Priority: High

Description: Bin Not cleared from my Ward

Image1

2.81 Mbit/s | 00:00:00 | 100.00 % | 10.08 KB / 10.08 KB

uncleared bin.jpg 10.08 KB

Image2

6.56 Mbit/s | 00:00:00 | 100.00 % | 10.08 KB / 10.08 KB

uncleared bin.jpg 10.08 KB

The ultrasonic bin level sensor shall be used to sense the distance from the mounting point to the bottom of the garbage bin or collection truck to measure fill levels. The sensor shall have in-built M2M communications capability for data transfer between sensor & server. Technical Specifications Applicable as below and as per Annexure

1. The sensor shall sense distance of minimum 3 meters.
2. The sensor data shall be used to obtain the fill level of the waste bins.
3. The sensor shall be IP67 rating (water & dust proof) and shall be capable to operate in conditions inside waste bins. These waste bins may contain solid waste, wet waste, industrial waste, or others as per the site conditions.
4. The sensor shall be easily mountable on the waste bin.
5. The sensor shall have supporting Lithium Ion battery pack with a minimum working life of 5 years.
6. The sensor should send automatic alarm to the server when the battery is about to run out of charge.

2.10. COMPONENT 10: Aurangabad Citizen Mobile Application and Website

A. Overview

All smart city components will have a mobile/browser facing interface. This will have a consolidated view which will be provided to public. This application should be able to provide all KPI's as applicable to public.

The Citizen app is a one-stop solution for citizens that bring to the citizen relevant, real time & interactive city information to help plan their day, and in turn seek (crowd source) inputs from citizens to enhance the services to serve the citizens.

A. Scope of Work

Citizens can use Citizen App to view real-time data on their mobile phones / tablets for a variety of details. Some of them include below information and may not be limited to this:

- Complaint registration & status tracking of any city services
- E- Governance all application intergration
- Free and paid Wi-Fi App
- Solid Waste Management System – Citizen Alert Mechanism
- Smart Transport System(ITS) & Smart Bus Stops integration with portal and Mobile App
- Special government messages to citizens, tourists on notification basis.
- Special services for citizens such as information on Voter ID and Aadhaar cards.
- Allows users to report Panic or danger which will be reported to the government and police officials for immediate help.
- Citizens / Tourists will also be provided with Current Weather information and Weather history on a date range and future weather information based on reliable weather sources.

B. Solution Requirement

- Application should have an appropriate administration interface to load information and track usage
- Application should have analytics installed to check the usage and functionality accessed
- Application should have notifications facility
- Application should be able to conduct poll as and when required.
- Application should be built in such a way that future integrations and enhancements can be done easily.
    - Mobile application be developed in Android and IOS (native)
    - Browser based application should be developed in general platforms as chosen by MSI and should have a responsive design to be opened on any mobile phone without distortion.
    - The application should have integration layer and should be able to pull information necessary from system
    - Application should have interface to all e-governance modules
    - Application should have SMS gateway integration
    - Application should have interface social media
    - Application should have bank interface for payment gateway

MSI shall provide Standard Operating Procedures (SOPs), and user Manuals a step-by-step instruction to operate and to resolve the situation quickly and easily.

Smartcity ASCDCL branding at appropriated and aesthetic location in APP website

Technical Specifications Applicable as per Annexure
Applicable Government Standards and guidelines must be follow.

Technical solution offer by MSI must complaint to Use cases as per annexure and provision for future addition to use cases

2.11. COMPONENT 11: Integration and Common Components

There are several ongoing projects in AMC that the MSI shall have tomake provision to integrate with. The following systems with the City Operation Command Centre:

- E-Governance System integrated with Citizen App
- Smart LED Lighting – Integrated with OCC
- GIS mapping for Aurangabad City across all components
- Smart Bus management system(ITS) and smart bus stop
- Wi-fi hot spot
- Vehicle tracking system for all solid waste management, ambulance or any other mulciple services vehicle
- Survelliance of city cameras
- Kiosk interface and management
- Any other system ASCDCL want to intergrate

A. Overview

Aurangabad has already awarded a contract to a 3rd party to implement LED based smart lighting solution through energy saving models, auto dimming technology, etc. MSI on-boarded under this RFP will be responsible for supporting the implementing agency and further integration of implemented smart lighting solution in the city to the OCC. It is estimated that there are about 40,000 street lights at present. The MSI may consider additional street lights for future integration into the OCC. Day-to-Day operational status of the Smart Lighting System should be visible in the OCC at all times.

B. Scope Of work

MSI shall be responsible for providing GIS map of Aurangabadcity which shall be a common platform across all solutions including City Wi-Fi, City Surveillance, Smart Bus Stop & Smart Transport, ICT enabled SWM, etc.

MSI shall also be responsible for appropriate geo referencing & geo tagging on the map covering all relevant assets like Wi-Fi Hotspots, bus stops, bus routes, bin locations, transfer stations, street poles, high masts, traffic signals, PA & VaMS systems etc

- GIS base IOP must have following layers
    - E-Governance System integrated with Citizen App
    - Smart LED Lighting – Integrated with OCC
    - GIS mapping for Aurangabad City across all components
    - Smart Bus management system(ITS) and smart bus stop
    - Wi-fi hot spot
    - Vehicle tracking system for all solid waste management, ambulance or any other mulciple services vehicle
    - Survelliance of city cameras
    - Kiosk interface and management

  GIS maps shall be comprehensive and detailed up to roads, houses and building level
- Solution shall ensure that the GIS Map provides complete details of the city in various digital vector layers and allows for zoom in/out, searching, and retrieving information capabilities.
- GIS details procured shall include the following data with attributes:
  - Road Network.
    - City Arterial Roads.
    - Streets
  - Administrative boundaries
    - District and Sub District Boundary.
    - Town Boundaries.
  - Building footprints and names
  - Points of Interest data to include:
    - Health services (Hospitals, Blood Banks, and Diagnostics centre, Ambulance Services, Other Medical Services, etc.)
    - Community services (fire stations, police stations, banks, ATMs, post offices, educational facilities, Govt. Buildings etc.)
    - Business Centres (Shopping malls, markets, commercial complexes etc.
    - Residential areas (Apartments, housing societies etc.)
    - Transportation (bus stops/Terminus, parking areas, petrol bunks, metro stations, seaports, airports etc.)

    - Recreation facilities (Restaurants, theatres, auditoriums etc.)
    - Other utilities such as travel and tourism facilities, religious places, burial grounds, solid waste locations etc.
    - Local landmarks with locally called names.
- Land-Cover
    - Green areas
    - Open Areas
    - Water bodies
- Address layers (Pin code, Locality, Sub-locality, House numbers/names)
- Geo referencing of all assets pertaining to the aforementioned solutions as required shall be provided by MSI
- All data procured shall be imported into a central database.

C. Solution Requirement

- System shall have capability to perform attribute or spatial queries on data from selected sources.
- System shall support Mobile platform, Android and Windows
- System shall support clipping and/or downloading of raster and vector data by authorised users.
- System shall support server side Geo-processing
- Application shall have standard and modern map navigation tools of pan and zoom.
- Application shall support client requests to print the spatial data.
- System shall be able to support industry-standard data types, industry-standard data formats, unlimited file size or database size, unlimited number of files or tables, and unlimited number of users.
- System shall support geocoding and reverse geocoding
- System shall allow the users to perform advanced spatial analysis like geocoding, routing, buffering and attribute based analysis.
- Application shall have standard and modern map navigation tools of pan and zoom.

- System shall have the facility wherein the user can opt to view in 2D or 3D environment.
- System shall be compatible with Google Maps, Bing™ Maps, Micro Station, AutoCAD, MGE, FRAMME, G/Technology, ODBC source.
- System shall support hierarchical legends, and watermarks
- Application shall allow users to view the data with different symbology styles like differentiating feature records based on attributes or types, dynamic label generation with conflict detection, and translucency of all raster data and area colour fill.
- System shall allow the user to find Address
- System shall be able to consume real-time enterprise published spatial data. It shall be able to consume the third-party published OGC web-services.
- Application shall be OGC compliant for database and shall provision conversion to other database formats.
- GIS base maps shall be installed on work stations at Command Control Centre and City Operation Centre. GIS maps and data replication shall happen from central system remotely.
- Provide GIS engine that shall allow operators to get an overview of the entire system and access to all the system components dynamically. GIS engine shall enable dynamic view of the location and status of resources and objects/sensors. System shall enable authorized users to open a new incident and to associate the incident with its geographic location automatically, via GIS display.

3. Testing and Acceptance Procedures

3.1. Testing and Acceptance Procedures

Testing and quality assurance in software development is more rigorous since each component has to be more reliable, if it is to be reused. A system is tested at various stages of development and deployment. For example, each component is tested as a unit for checking the correctness of its own code. The component shall be tested with its dependent components. After final release of the entire set of components, system is tested for the correctness of system functionality. The components shall be tested in simulated production load for performance and load analysis. The MSI along with consortium partners shall be responsible for the testing processes such as **planning** (includes preparing test plans and defining roles and their responsibilities), **preparation** (consists of preparing test specification, test environment and test data) and **execution** (includes testing at various levels like unit level, integration level, system level and production).

A. Test Plan

Test plans are prepared for each phase of testing. The initial test plan is created during the Project Planning phase. The initial test plan describes who performs which type of testing and when. Ideally master test plan covers all types of test i.e. from unit testing to production testing. The MSI along with consortium partners is expected to submit the test plans to ASCDCL for approval. Any changes made to the test plan during the project life cycle should be communicated to ASCDCL for approval. Test plans should contain following items:

- Roles and responsibilities of test team
- Approach to testing
- Function testing
- Security testing
- User Interface and reports testing
- Concurrency testing
- Performance and Load testing
- Test Scenarios along with entry and exit criteria
- Test specifications
- Suspension and resumption criteria

B. Test scenarios

The MSI along with consortium partners should prepare test scenario for each business scenario. A test scenario when executed should fulfil a business requirement as per the scope of business functionality. Test scenarios shall include following:

- Test Specification - During the test specification phase, the test cases are specified. It consists of description of the input, process to be executed and a prediction of output results.
- Test Environment - Component developer does unit testing and integration testing. Integration testing can be delegated to a specialized testing group. Each of the members in the testing group is provided with testing environment according to his/her role and responsibilities. Following is sample testing environment for testing:
    - A workstation
    - A set of tools and applications required on workstation like access to user interface, browser etc.
    - Access to centralized document database (where all the project related documents are maintained)
    - Access to testing tools and defect logging tools
    - Access to the central database or repository for development and unit testing (this database contains sample test data)
    - Access to deployed components
- Test Data - Test data is prepared for testing at each stage. The test data should be prepared in such a way that it covers basic path and every alternate path of the code. The basic path and alternate paths are prioritized to capture relevant data. Tools can also be used to generate test data.

C. Test Execution

The following testing steps are usually employed in the project lifecycle. The MSI along with consortium partners expected to follow these steps.

Unit Testing: In unit testing, each piece of code has to be rigorously tested. At this stage testing is done according to the priority of path of code. All the test results are logged in the defect logging tools. After completion of testing, code is corrected for defect logs. This process is iterative till criteria for successful testing is reached.

Integration Testing: Upon completion of unit testing, integration testing begins. The purpose is to ensure distinct components of the application still work in accordance to customer requirements. Test sets will be developed with the express purpose of exercising the interfaces between the components. This activity is to be carried out by the Test Team. Integration test will be termed complete when actual results and expected results are either in line or differences are explainable/acceptable based on client input.

Incremental Integration Testing: Continuous testing of an application as new functionality is added.

System Testing: System testing is performed when all the components are delivered to central repository prior to the release of the software. The testing is done on priority basis of business processes. All the defects are logged and assigned to respective component owners. The component and unit testing shall be performed after the correction of code. However, it may depend on size and type of individual test specifications. Impact analysis is useful to narrow done testing efforts by identifying critical test cases affected due to code change.

Pre-Production Testing: Pre-Production testing is done simulating the production load. Test data is either prepared or generated from the tools. This testing is used to evaluate performance, load capacity and concurrency. Load testing tools can also be used for this purpose. Following special type of testing are done during Pre-production Testing Phase:

Regression Testing: The objective of regression testing is to ensure software remains intact. A baseline set of data and scripts will be maintained and executed to verify changes introduced during the release have not “undone” any previous code. Expected results from the baseline are compared to results of the software being regression tested. All discrepancies will be highlighted and accounted for, before testing proceeds to the next level.

Performance Testing: Although performance testing is described as a part of system testing, it can be regarded as a distinct level of testing. Performance testing will verify the load, volume, and response times as defined by requirements.

Load Testing: Testing an application under heavy loads, such as the testing of a web site under a range of loads to determine at what point the systems response time degrades or fails.

Installation Testing: Testing full, partial, or upgrade install/uninstall processes. The installation test for a release will be conducted with the objective of demonstrating production readiness. This test is conducted after the application has been migrated to the client’s site. It will encompass the inventory of configuration items (performed by the application’s System Administration) and evaluation of data readiness, as well as dynamic tests focused on basic system functionality. When necessary, a sanity test will be performed following the installation testing.

Security/Penetration Testing: Testing how well the system protects against unauthorized internal or external access, wilful damage, etc. This type of testing may require sophisticated testing techniques.

Recovery/Error Testing: Testing how well a system recovers from crashes, hardware failures, or other catastrophic problems.

Acceptance Testing: During the test scenarios definition, for each of the business scenario,an acceptance criterion is defined. Acceptance criteria include expected behaviour of the s/w component and the expected results (data). Expected results form a part of the Exit Criteria. In addition to expected result and behaviours, some conditions are also specified in the exit criteria. They can be:

- Number of bugs to be discovered for a functional module. This depends on size of the functionality and is an indicator of amount of testing done. If any medium or low-priority errors are outstanding - the implementation risk must be signed off as acceptable by ASCDCL and Lead Partner along with consortium partners
- All High Priority errors from System Test must be fixed and tested by MSI along with consortium partners needs to get the acceptance criteria approved from ASCDCL for all the functional components of the system. The Acceptance Criteria for each release into production environment will be agreed upon by MSI along with consortium partners in consultation with ASCDCL prior to release from Testing to production environment. After installation, if any bug is reported or there is non-compliance to requirements then a proper procedure should be followed. End-user should report (“Change Request”) to his/her supervisor about the bug that will in turn get forwarded to Project Manager (PM). PM will forward the List of change request to Lead Partner along with consortium partners. After the bug is fixed, it should be reflected in the production copy after testing it.

Performance Testing: The MSI has to test and demonstrate the operational performance requirement as per specification after completion of entire scope. This will be part of acceptance testing. The system will be taken over by owner only after successful operational performance testing. The MSI has to arrange necessary hardware / software to demonstrate the performance testing. MSI should note that ASCDCL can appoint a third party agency for conducting any part of above testing procedures (in addition to the testing carried out by the Bidder).

D. Testing, Commissioning & Successful Operation:

The scope includes testing and commissioning & implementation of all equipment, sub-systems and systems of the project and putting them into successful technical & commercial operation. The scope shall include but not limited to the requirements given elsewhere in the specification. The MSI shall be responsible to provide all necessary testing and commissioning personnel, tools/kits, test equipment etc.

4. Hand holding and Training

4.1. Handholding and Training:

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

- MSI shall prepare and submit detailed Training Plan and Training Manuals to ASCDCL /authorized entity for review and approval.
- Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
- MSI shall be responsible for necessary demonstration environment setup of all ICT solutions in this RFP to conduct end user training. End user training shall include all the equipment including but not limited to all the applications and infrastructure at Operation centres, data centres & field Locations. End user training shall be conducted at a centralized location or any other location as identified by ASCDCL with inputs from MSI.
- MSI shall conduct end user training and ensure that the training module holistically covers all the details around hardware and system applications expected to be used on a daily basis to run the system.
- MSI shall impart operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
- MSI shall prepare the solution specific training manuals and submit the same to Authority for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
- MSI shall provide training to selected officers of ASCDCL covering functional, technical aspects, usage and implementation of the products and solutions.
- MSI shall ensure that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
- An annual training calendar shall be clearly chalked out and shared with ASCDCL along with complete details of content of training, target audience for each year etc.

- MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
- MSI shall ensure that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by MSI.
- Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by MSI.
- Time Schedule and detailed program shall be prepared in consultation with ASCDCL and respective authorized entity (Police). In addition to the above, while designing the training courses and manuals, MSI shall take care to impart training on the key system components that are best suited for enabling the personnel to start working on the system in the shortest possible time.
- MSI is required to deploy a Master Trainer who shall be responsible for planning, designing and conducting continuous training sessions.
- Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.
- ASCDCL shall be responsible for identifying and nominating users for the training. However, MSI shall be responsible for facilitating and coordinating this entire process.
- MSI shall be responsible for making the feedback available for the Authority/authorized entity to review and track the progress, in case, after feedback, more than 30% of the respondents suggest that the training provided to them was unsatisfactory or less than satisfactory then the MSI shall re-conduct the same training at no extra cost.

Types of Trainings

Following training needs is identified for all the project stakeholders:

I. Basic IT training

This module shall include components on fundamentals of:

- Computer usage,
- Network,
- Desktop operations,
- User admin,

- Application installation,
- Basic computer troubleshooting etc.

II. Functional Training

- Basic IT skills
- Software Applications (City Operation Centre and Command & Control Centre)
- Networking, Hardware Installation
- Centralized Helpdesk
- Feed monitoring

III. Administrative Training

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

IV. Senior Management Training

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

Post-Implementation Training

- Refresher Trainings for the Senior Management as an when required
- Functional/Operational training and IT basics for new operators
- Refresher courses on System Administration
- Change Management programs

Term Completion Handover Training

At the end of the 5 Year O&M term, the MSI will be either granted an extension or will be required to hand over the system to a new operator. It is imperative that the MSI creates the provision for a smooth handover.

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

5. Project Implementation Timelines & Deliverables

ASCDCL intends to implement the project in phased manner approach, distributed in three phases as mentioned below:

5.1. Phase I – T + 1 months (T is the date of signing of the contract with MSI)

I. Study& Reporting Activities

A	**Phase I: Mobilization, Design**	T + 1 months
1	**Resource Mobilization**	T + 1 months
2	Detailed Project Study for all ICT solution: a) Detailed Survey of identified Sites, Network and Power Requirements b) Hardware and Software Deployment plans c) Detailed Project Plan including Operations management, Contract management, Risk Management, Information Security and Business Continuity d) FRS, SRS, SDD Documents for all work streams & components	T + 1 Months T + 1 months

5.2. Phase II – T + 6 months

B	**Phase II: Supply, Installation, and Integration**	**T + 6 months**
1	City Communication Network	T + 6 Months
2	Command and Control Centre (CCC) for Police	T + 6 Months
3	City Operation Command Centre (OCC) for AMC	T + 6 Months
4	CCTV based City Surveillance System	T +6 Months
5	Biometric Attendance System	T + 2 Months
6	Smart Transport System & Smart Bus Stops	T + 6 Months
7	City Wi-Fi Spots	T + 6 Months
8	Digital Display Signage	T + 4 Months
9	ICT Enabled Solid Waste Management	T + 6 Months

10	Smart Traffic Management System	T + 6 Months
11	Aurangabad Citizen Mobile Application & Website/Portal	T + 6 Months
12	Integration Components	T + 6 Months

5.3. Phase III – T + 7 months

C	**Phase III: Testing & Go Live**		T+7 Months
1	Functional Testing	Compliance Report	T+7 Months
2	Operations Testing	Compliance Report	T+7 Months
3	Load and Failover Testing	Compliance Report	T+7 Months
4	Go Live		T+7 Months

5.4. Phase IV – T1 + 60 months (T1 is the date of Go Live of all application)

D	**Phase IV: Operations & Maintenance phase for a period of 60 months from the date of Go Live**		
1	Operation & Maintenance	SLA Compliance Report	Every Quarter

6. Bill of Quantities (BOQ)

6.1. Command Control Center

Sr. Nos	Description of Item	UoM	QTY
1	Video Wall (along with hardware & software) Solution - 9 x 3 Display	Set	1
2	Projector for Meeting Room	nos	1
3	Fire & Smoke Detectors	LS	LS
4	Laser Colour Printers	nos	2
5	3 Screen -Operators Client Workstations for Command Control Center	nos	25
6	L2 Switch - 48 port	nos	As Required
7	UPS Online with Battery	nos	1
8	Air Conditioning	nos	As Required
9	CCTV camera	nos	As Required
10	Biometric access control system	nos	Per Room
11	Operating System Licence	nos	As Required
12	Networking & cabling	LS	As Required
13	Gen Set	nos	1
14	IP phones	nos	0
15	IBMS Solution	nos	0
16	IP soft phones	Nos	0
17	Video Phone	nos	0
18	Voice Logger for Phones- For Forensic	nos	0
19	Screen Recording-Software /Hardware (Forensic)	nos	0
20	Implementation services (Installation & Commissioning)	LS	LS

6.2. Data Center

Sr. Nos	Description of Item	UoM	QTY
1	Smart Rack solution of min 6 racks for data centre with Accessories, with complete electrical connections, PAC precision Air-condition, fire retardant, access control	set	1
2	Core Router	nos	As per requirement
3	Internet Router	nos	As per requirement
4	Firewall and IPS/IDS	nos	4
5	Core Switch (L3)	nos	2
6	L2 Switch -48 Port	nos	As per requirement
7	San Switch	nos	As per requirement
8	Storage - 1.25 PB Usable	nos	1
9	Anti-virus Suite / Gateway	nos	1
10	Back up s/w	nos	0
11	LTO (Back Up Drives)	nos	0
12	Blade chassis	nos	2
13	Blade Server	nos	32
14	Virtualization Software	nos	1
15	APT, SIEM, DLP, ADC, EDR	nos	1 each
16	Data Center Site Preparation	nos	As per requirement
17	SLA, Helpdesk& EMS Solution	LS	As per requirement
18	Firewall (WAF)	nos	0
19	Furniture Items and chairs etc as per approved design	LS	As per requirement
20	Server License	LS	As per requirement
21	DB License	LS	As per requirement
22	Implementation services (Installation & Commissioning)	LS	LS

6.3. Operation Command Center

Sr. Nos	Description of Item	UoM	QTY
1	Smart Rack solution for data center with Accessories, with complete electrical connections, PAC precion Aircondition, fire retardent, access control	set	1
2	Video Wall (along with hardware & software) Solution - 6x3 Display	Set	1
3	Projector for Meeting Room	Nos	1
4	Fire & Smoke Detectors	Nos	LS
5	Colour Printers	Nos	1
6	Internal and External Firewall and IPS/IDS	Nos	As Required
7	3 Screen -Operators Client Workstations for Command Control Center	Nos	15
8	L2 Switch -48 Port	nos	As per requirement
9	San Switch	nos	As per requirement
10	Storage DAS- 500 TB Usable	nos	1
11	Anti virus Suite / Gateway	nos	1
12	Back up s/w	nos	1
13	Blade chassis	nos	2
14	Blade Server	nos	20
15	Virtualization Software	nos	1
16	APT,SIEM,DLP,ADC,EDR	nos	1
17	Data Center Site Preparation	LS	As per requirement
18	SLA, Helpdesk& EMS Solution	nos	As per requirement
19	Firewall (WAF)	nos	As per requirement
20	Server License	LS	As per requirement
21	DB License	LS	As per requirement
22	L2 Switch - 48 port	Nos	As Required
23	UPS Online with Battery	Nos	1
24	Air Conditioning	Nos	As Required
25	CCTV camera	Nos	As Required
26	Biometric access control system	Nos	Per Room
27	Operating System Licence	Nos	As Required
28	Networking & cabling	Nos	As Required
29	Gen Set	Nos	1
30	IBMS Solution	Nos	1
31	Implementation services (Installation & Commisioning)	LS	LS
32	Furniture Items and chairs etc as per approved design	1	1

Sr. Nos	Description of Item	UoM	QTY
33	City Operations Platform - IoT Platform/Data Normalization software & City Operation Centre Software	LS	1
34	Integration of various sensors, applications/systems	LS	1

6.4. Utility Poles Passive and active components

Sr. Nos	Description of Item	UoM	QTY
1	UTILITY Poles with accessories provisions for Environmental Sensors, CCTV camera, Wi-Fi, and junction box	Nos	519
2	Junction Box	Nos	519
3	POE Industrial switch	Nos	519
4	Implementation services (Installation & Commissioning)	Nos	1

6.5. ITMS

Sr. Nos	Description of Item	UoM	QTY
1	Mobile application	Nos	0
2	Traffic engineering services	Nos	0
3	Implementation services (Installation & Commissioning)	LS	0

6.6. Smart Bus Stop

Sr. Nos	Description of Item	UoM	QTY
1	GPS Device for city buses	Nos	0
2	Passenger Information System (32” Industrial Grade LED TV)	Nos	57
3	LED Display in City buses type 1	Nos	0
4	LED Display in City buses type 2	Nos	0
5	LED Display in City buses type 3	Nos	0
6	Display controller and Panel	Nos	0
7	PA system	Nos	0
8	Surveillance Camera (Network IR Bullet Camera) 5 nos per bus	Nos	0
9	Digital outdoor Display	Nos	0
10	Smart BUS Stops	Nos	57
11	Smart Transport Application Server	Nos	1
12	Vehicle Scheduling and Despatch System	Nos	1
13	Incident Management System	Nos	1
14	Web Portal for bus schedule, bus route and ETA	LS	As per requirement
15	Mobile Application	LS	As per requirement
16	Integration with Smart City Dashboard	LS	As per requirement

Sr. Nos	Description of Item	UoM	QTY
17	Phase-1 Implementation services (Installation & Commissioning)	LS	As per requirement

6.7. ICT enabled Waste Management Software

Sr. Nos	Description of Item	UoM	QTY
1	Vehicle Tracking System (VTS) GPS Device	nos	0
2	Hand held GPS for push carts/Tricycle	nos	0
3	RFID receiver for Auto tippers	nos	As per requirement
4	RFID Tagging for Tippers (Waste Treatment Plant)	nos	As per requirement
5	RFID Receiver with all accessories at weigh bridge &entry point	nos	As per requirement
	RFID receiver with all accessories at exit point	nos	As per requirement
	FIX Camera	nos	1
	ICT enabled Waste Management Software	nos	As per requirement
6	Mobile Application	LS	As per requirement
7	Integration with existing Map	LS	As per requirement
8	Weigh bridge and integration application	Nos.	4
9	Implementation services (Installation & Commissioning)	LS	As per requirement

6.8. WIFI

Sr. Nos	Description of Item	UoM	QTY
1	Wireless Controller	Nos	1
2	Access Points	Nos	700
3	Application	Nos	1
4	Authentication server	Nos	1

6.9. Digital Outdoor Display and Kiosk

Sr. Nos	Description of Item	UoM	QTY
1	Digital outdoor Display	Nos	50
2	Indoor touch Kiosks	Nos	10
3	Indoor Non Touch Kiosks	Nos	50
4	content manager server	Nos	1
5	Application	Nos	1
6	Authentication server	Nos	1
7	Gantry	Nos	50
8	Implementation services (Installation & Commissioning)	LS	1

6.10. E Office

Sr. Nos	Description of Item	UoM	QTY
1	IP Phone	Nos	0
2	Video Phones	Nos	0
3	IP Telephony system	Nos	0
4	Softphone licenses for PA, ECB, Desktop/Laptop	Nos	0
5	Face recognition Attendance devices	Nos	
6	Biometric Devices	Nos	30
7	Hand held biometric devices	Nos	50
8	Network switched L2 48 port poe	Nos	0
9	Implementation services (Installation & Commissioning)	ls	1
10	Smart Rack solution for data centre with Accessories, with complete electrical connections, PAC precision Air-condition, fire retardant, access control	set	0

6.11. End points like cameras, ECB, PA

Sr. Nos	Description of Item	UoM	QTY
1	FIX BOX Camera	Nos	600
2	RLVD Camera	Nos	0
3	ANPR Camera	Nos	0
4	Evidence camera	Nos	0
5	PTZ camera	Nos	100
6	FRS camera	Nos	0
7	MOBILE ANPR setup	Nos	0
8	IP PA system	Nos	0
9	IP ECB box	Nos	0
10	Implementation services (Installation & Commissioning)	LS	1

6.12. Licenses

Sr. Nos	Description of Item	UoM	QTY
1	**Video Analytics Software and Licences**	Nos	700
2	Video Management Software	Nos	1
3	Video Management Software and Camera Licenses	Nos	700
4	Forensic Software & Licenses	Nos	0
5	Implementation services (Installation & Commissioning)	LS	1

6.13. SETUP at Local Police Station

Sr. Nos	Description of Item	UoM	QTY
1	Three monitor work station	Nos	20
2	UPS	Nos	20
3	Furniture	Nos	20
4	AC	Nos	20
5	Implementation services (Installation & Commissioning)	LS	1

6.14. Project Management & Infrastructure Set-up

Sr. Nos	Description of Item	UoM	QTY
1	Control Room Site Preparation covering Partitioning, Enclosures, Earthing, Power Cabling etc. (safety)	LS	
2	Cubicles with Table and Chair for operators (As required) - for operators	LS	
3	Detailed systems/site wise survey study of above Systems	As Required	
4	Any other Installation, Configuration and Customization for complete project	As Required	
5	Capacity Building and Administrative Expenses	As Required	
6	Another item (if Required)		

6.15. Price component for OPEX

S.No.	Subsystems / Items	UoM	QTY
1	Price component for OPEX	**LS**	
2	Network as Service	**LS**	
3	Technical & Operational Manpower Cost after Installation	**LS**	
4	Electrical Charges	**LS**	
5	City Operations Centre / City Command Center Utility & Miscellaneous Charges (Telephone, Local Conveyance, Local Office, Utilities, etc.)	**LS**	
6	Data Center as colocation	**LS**	
7	DR – Cloud Based for 5 Years	**LS**	
8	Intelligent Transport system (ITS) for Bus stop	**LS**	
9	GPS services for SWM	**LS**	
10	Helpdesk (CCC and City Operation Center)	**LS**	
11	Project Implementation price	**LS**	
12	Handholding and Training price	**LS**	
13	Operation & maintenance resources	**LS**	
14	Operations & Maintenance for IT / Non-IT Infrastructure for 5 Years	**LS**	
15	Insurance + Annual Maintenance Cost	**LS**	
16	Any other price item not included above (if Required)	**LS**	
17	One Time DR Migration Cost	**LS**	

Annexure- Technical Specification Requirements

(* The specifications provided in this RFP are indicative and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

Annexure 1 – Network Backbone

(* The specifications provided in this RFP are indicative Minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation**)**

Network Backbone				
S.No	**Parameter**	**Minimum Specifications or better**	**Compliance (YES/NO_**	**Deviations/Remarks**
CN-001	Provider should have co-location facilities	for Hosting of Disaster recovery data centre		
CN-002	Customisations	Service provider must offer flexible technical solution to meet smart city requirements		
CN-003	NOC	for Network monitoring for performance and uptime at CCC and OCC		
CN-004	uptime	99.98% uptime SLA required		

Annexure 2 -Command Control Center (CCC) For Police & City Operation Command Center(OCC) for AMC

(* The specifications provided in this RFP are indicative Minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

2.1 Laser Video Wall

S.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
VWCCC.REQ.001	General	Cube & controller should be from the same manufacturer		
VWCCC.REQ.002	Video wall	50'' Cubes (LASER) Based projection)		
		- 9X3 for Command Control Centre		
		- 6X3 for OCC		
VWCCC.REQ.003	Technology	Single chip DLP Technology		
VWCCC.REQ.004	Resolution	1920x1080		
VWCCC.REQ.005	Brightness	Minimum 2200 lumens		
VWCCC.REQ.006	Dynamic Contrast	1000000:1 or more		
VWCCC.REQ.007	Display technology	DLP rear projection with DMD Chip		
VWCCC.REQ.008	Colour gamut	>15 mill		
VWCCC.REQ.009	Brightness uniformity	≥ 98 %		
VWCCC.REQ.010	Screen	180° viewing angle screen		
VWCCC.REQ.011	Screen Gap	≤ 0.2 mm		
VWCCC.REQ.012	Colour stability	Self-calibration with advanced color sensor		
VWCCC.REQ.013	Dimensions	Diagonal: 50 " or better		
VWCCC.REQ.014	Light Source Type	Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes.		
VWCCC.REQ.015	Light source lifetime	Eco Mode: 100,000 hours		

S.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
		Normal Mode: 80,000 hours		
VWCCC.REQ.016	Conditions for operation	as per site condition requirements		
VWCCC.REQ.017	Control BD Input terminals	Input: 1 x Digital DVI		
		Input: 1 x HDMI		
		Input: 1 x Analog RGBHV		
		Output: 1 x Digital DVI		
VWCCC.REQ.018	Direct Ethernet access	IP control		
VWCCC.REQ.019	Graphical user interface	All settings and operational parameters		
VWCCC.REQ.020	Dust Proof Projection Engine	Projection system designed to meet IEC/ EN-60529 (IP6X standard)		
VWCCC.REQ.021	Certification	Should be BIS certified		
VWCCC.REQ.022	Maintenance Access	Rear Maintenance		
VWCCC.REQ.023	Cube control & Monitoring	Videowall should be equipped with a cube control & monitoring system		
		System should be based on Python- Django framework with web browser architecture or better		
		Should be able to control & monitor individual cube, multiple cubes and multiple video walls		
		Provide videowall status including Source, light source, temperature, fan and power information		
		Should provide a virtual remote on the screen to control the videowall		

S.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
		Input sources can be scheduled in " daily", "periodically" or "sequentially" mode per user convenience		
		System should have a quick monitor area to access critical functions of the videowall		
		User should be able to add or delete critical functions from quick monitor area		
		Automatically launch alerts, warnings, error popup windows in case there is an error in the system		
		User should be able to define the errormessages as informational, serious or warning messages		
		Automatically notify the error to the administrator or user through a pop up window and email		
		Status log file should be downloadable in CSV format as per user convenience		

2.2Video Wall Controller

Sr.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
VWC.REQ.001	Display controller	Redundant Controller to control OCC and CCC video wall		
VWC.REQ.002	Chassis	19" industrial Rack mount		
VWC.REQ.003	Operating System Platform	Window 7- 64 bit or Linux		
VWC.REQ.004	Processor options	Xeon/ i3/i5/ i7		
VWC.REQ.005	RAM	Std. 4 GB DDR3, higher on request		
VWC.REQ.006	HDD	Support up to minimum 2 HDD		
		Std.: 1 TB , can be upgraded on request		
VWC.REQ.007	Networking	Dual-port Gigabit Ethernet Controller inbuilt Supports Add on copper/ optical fiber adapters		
VWC.REQ.008	Input / Output supported	Serial ATA * 2x RJ45 LAN ports USB 2.0 port		
VWC.REQ.009	Power Supply	(1+1) Redundant hot swappable		
VWC.REQ.010	Cooling	should be capable of keeping unit in range of operating temperature range		
VWC.REQ.011	Indicators	LED's for HDD activity and Power status		
VWC.REQ.012	Switches	Power On/Off and System Reset		
VWC.REQ.013	Monitoring options	CPU, FAN, Temperature		
VWC.REQ.014	Accessories	DVD +RW ,Keyboard and mouse		
VWC.REQ.015	Voltage	100-240V @ 50/60 Hz		
VWC.REQ.016	Redundancy support	Power Supply, HDD, Cooling FAN, LAN ports		

Sr.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
VWC.REQ.017	Scalability	Display multiple source windows in any size, anywhere on the wall		
VWC.REQ.018	Control functions	Brightness / contrast / saturation/ Hue/ Filtering/ Crop / rotate		
	Accessories	DVD-R,DVD+RW,, Keyboard, mouse		
VWC.REQ.019	Power Supply	(1 + 1) Redundant AC-DC high-efficiency power supply		
		* AC Voltage 100 - 240V, 50-60Hz		
VWC.REQ.020	Operating Conditions	As per site condition		

2.3 Integrated Building Management System (iBMS)

S.No.	Specifications
A	**Solution for iBMS:** Solution should provide a 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). System should have the service dependency engine that allows to take intelligent decisions, as per the business needs/requirements. The tool should have the service oriented architecture layer and the mediation layer in a single plane. iBMS should be open for third party integration via (soap, xml, web service, snmp-v1, v2,v3). NO/NC ports (IO ports) and Modbus (TCP/IP&RTU) integration should be standard. For other industrial protocols, gateway integration should be available. Solution should perform the following general functions. Should be scalable with ready device certifications to accommodate new infrastructure getting added to the building.
1	**Visibility –** It should get a single platform to manage the entire building and its components. 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.
2	**Capacity Planning -** 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 areas which may need to be upgraded/downgraded (cooling, power, storage, etc.) with time. All MSI (end equipment vendors) SLA's and their respective maintenance contracts would be part of the OMS (operations and maintenance) plan.
3	**Third Party Integration -** Seamless Data Sharing to build a "Collaborative Decision-Making System".
4	**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.
5	**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.
6	**Root-Cause Analysis -** Isolate and pinpoint problem area before it impacts the building operations & business continuity while suppressing down the unwanted events.

S.No.	Specifications
7	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.
8	System should be capable enough to store the raw data or as polled data, for at-least for 365 days. It should also have the facility to automate the backup process or allow to take manual backup, in case if it is required.
9	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.
10	Support for email and SMS both (integration with SMS-gateway & GSM communication).
B	**Energy Management**
1	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.
2	System should be able to continuously monitor the quality of power, supplied to the electricity board and by the Generators (PF, frequency, harmonics distortion etc.), to avoid downtime.
3	System should have the feature to setup thresholds on each of the monitored energy parameter.
4	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, to avoid any breakdown.
C	**Fire Alarm System Monitoring and Management**
1	Should proactively alert in case of electrical fire (short circuit or over current)
2	System should have the capability to integrate with different makes of fire alarm systems in the DCs and provide alarms generated by system on Central Dashboard.
3	System should be able to plan and process a proper evacuation plan in case of fire
4	Trigger Audio and Visual alarm
5	Co-relate with the nearest camera in the site with the zone of the FAS.
6	Switching ON of lights on the evacuation pathway.
D	**Centralized Reporting & Dashboard**
1	Dashboard and reporting engine should provide centralized view for the entire infrastructure (physical security, safety & energy) in the building.
2	It should provide business users with highly interactive and power-users with highly sophisticated, pixel-perfect reports.
3	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.

S.No.	Specifications
4	It should provide Analysis to explore data by multiple dimensions such as customer, product, network and time into the hands of business users.
5	It should provide Intuitive & rich graphic designer to create customized reports, such as: DC-PUE (enables to measure how much energy is getting consumed in IT and how much in DC infrastructure).
6	Solution should provide a comprehensive centralized dashboard for health monitoring of DC (Infrastructure) components like: Electrical Panels, PAC, UPS, DG, Fuel etc.)
E	**DG Monitoring**
1	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.
2	System should be capable to do fuel level monitoring of diesel tanks installed for gensets in the DC/DR building, to have a proactive estimation of fuel availability.
3	Parameters - Generator and Fuel Supply Automation ▪ Mains Fail ▪ DG On ▪ DG Failed to start / DG Failed to stop ▪ DG Fuel Level Low ▪ High Water Temperature / High Coolant Temperature ▪ Low Battery Voltage ▪ Low Lube Oil Pressure(LLOP) ▪ Automate Fuel Supply Process to reduce fuel consumption cost.

2.4 Monitoring Workstations/Desktop

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MONW.001	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better		
MONW.002	Chipset	Latest series 64bit Chipset		
MONW.003	Motherboard	OEM Motherboard		
MONW.004	RAM	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC		
MONW.005	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)		
MONW.006	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.		
MONW.007	Media Drive	NO CD / DVD Drive		
MONW.008	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.		
MONW.009	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)		
MONW.010	Ports	Minimum 6 USB ports (out of that 2 in front)		
MONW.011	Keyboard	104 keys minimum OEM keyboard		
MONW.012	Mouse	2 button optical scroll mouse (USB)		
MONW.013	PTZ joystick controller *(with 2 workstations in CCC)*	▪ PTZ speed dome control for IP cameras ▪ Minimum 10 programmable buttons ▪ Multi-camera operations ▪ Compatible with all the camera models offered in the solution ▪ Compatible with VMS /Monitoring software offered		
MONW.014	Monitor	Three 22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
MONW.015	Certification	Energy star 5.0/BEE star certified		
MONW.016	Operating System	64 bit pre-loaded OS with recovery disc		
MONW.017	Security	BIOS controlled electro-mechanical internal chassis lock for the system.		
MONW.018	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)		
MONW.019	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.		

2.5 Network Laser Colour Printer

Sr. No.	Item	Minimum Specifications or better	Compliance (Yes / No)	Deviations / Remarks
NLCP.001	Print Speed	Black: 15 ppm or above on A3, 24 ppm or above on A4 Colour: 8 ppm or above on A3, 12 ppm or above on A4		
NLCP.002	Resolution	600 X 600 DPI		
NLCP.003	Memory	Min. 8 MB or more		
NLCP.004	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes		
NLCP.005	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray		
NLCP.006	Duty Cycle	25,000 sheets or better per month		
NLCP.007	OS Support	Linux, Windows 2000, Vista, 7, 8, 8.1		
NLCP.008	Interface	Ethernet Interface		

2.6KVM Module

Sr. No.	Item	Minimum Specifications or better	Compliance (Yes / No)	Deviations / Remarks
KVMM.001	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre		
KVMM.002	Form Factor	19” rack mountable		
KVMM.003	Ports	minimum 8 ports		
KVMM.004	Server Connections	It should support both USB and PS/2 connections.		
KVMM.005	Auto-Scan	It should be capable to auto scan servers		
KVMM.006	Rack Access	It should support local user port for rack access		
KVMM.007	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
KVMM.008	OS Support	It should support multiple operating system		
KVMM.009	Power Supply	It should have dual power with failover and built-in surge protection		
KVMM.010	Multi-User support	It should support multi-user access and collaboration		

2.7Online UPS

Sr. No.	Item	Minimum Specifications or better	Compliance (Yes / No)	Deviations / Remarks
ONUPS.001	Capacity	Adequate capacity to cover all above IT Components at respective location		
ONUPS.002	Output Wave Form	Pure Sine wave		
ONUPS.003	Input Power Factor at Full Load	>0.90		
ONUPS.004	Input	Three Phase 3 Wire for over 5 KVA		
ONUPS.005	Input Voltage Range	305-475VAC at Full Load		
ONUPS.006	Input Frequency	50Hz +/- 3 Hz		
ONUPS.007	Output Voltage	400V AC, Three Phase for over 5 KVA UPS		
ONUPS.008	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		
ONUPS.009	Inverter efficiency	>90%		
ONUPS.010	Over All AC-AC Efficiency	>85%		
ONUPS.010	Over All AC-AC Efficiency	>85%		
ONUPS.011	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage, 2) Output under voltage, 3) Battery low, 4) Inverter overload, 5) Over temperature, 6) Output short		
ONUPS.012	Battery Backup	30 minutes in full load		
ONUPS.013	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery		
ONUPS.014	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		

Sr. No.	Item	Minimum Specifications or better	Compliance (Yes / No)	Deviations / Remarks
ONUPS.015	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
ONUPS.016	Cabinet	Rack / Tower type		
ONUPS.017	Operating Temp	0 to 50 degrees centigrade		
ONUPS.018	Management Protocol	SNMP Support through TCP/IP		

2.8 DG Set

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DGS.001	General Specifications	▪ Auto Starting DG Set mounted on a common base frame with AVM (Anti-Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions. ▪ KVA rating as per the requirement		
DGS.002	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS5514/ ISO 3046/ IS 10002		
DGS.003	Fuel	High Speed Diesel (HSD)		
DGS.004	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.		
DGS.005	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators ▪ Incoming and outgoing voltage / Current in all phases ▪ Frequency, KVA and power factor ▪ Time indication for hours/minutes of operation ▪ Fuel Level in fuel tank, low fuel indication ▪ Emergency Stop button ▪ Auto/Manual/Test selector switch ▪ MCCB/Circuit breaker for short-circuit and overload protection ▪ Control Fuses, Earth Terminal ▪ Any other switch, instrument, relay etc. essential for Automatic functioning of DG set with AMF panel		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DGS.006	Acoustic Enclosure	▪ DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). ▪ Enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand Aurangabad climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangement, complete and		
DGS.007	Fuel Tank Capacity	It should be sufficient & suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.		

2.9Structured Cabling Components &Electrical cabling component

Structured Cabling Components:				
Sr. No.	**Item**	**Minimum Specifications or better**	**Compliance** **(Yes / No)**	**Deviations / Remarks**
SCC.001	Standards	ANSI TIA 568 C for all structured cabling components		
SCC.002	OEM Warranty	OEM Certification and Warranty of 15-20 years as per OEM standards		
SCC.003	Certification	UL Listed and Verified		

Electrical cabling component:				
Sr. No.	**Item**	**Minimum Specifications or better**	**Compliance** **(Yes / No)**	**Deviations / Remarks**
ECC.001	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's		

2.10 Integrated Operation Platform (IOP)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IOP.001	General Requirements	IOP shall be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform		
IOP.002	General Requirements	IOP system shall provide a real time Common Operating Picture (COP) of the area involving all agencies using a simple GUI		
IOP.003	General Requirements	Some of incidents that IOP responds to include but are not limited to the following: · Hazards / Calamities: Natural, Man-made, Environmental · Epidemics (Health) · Transportation (Road, Rail etc) · Public Utility (Water, Electricity, Street Lighting, Solid Waste Management) · Public Safety (Crime, Law & Order)		
IOP.004	General Requirements	System shall integrate with various emergency response services such as Ambulance, Fire, Disaster Management Systems, etc.,		
IOP.005	General Requirements	System shall integrate with RSS feeds from various news alert like Yahoo, Times etc and event can be possible to generate in IOP on keyword receive from such RSS feeds s		
IOP.006	General Requirements	System shall support various sensors like Cameras, GPS, Voice devices (Analog & Digital), Storage devices, Sensor inputs from other applications/ systems		
IOP.007	General Requirements	System should provide tool to define/create any event/rule based Standard Operating Procedure (SoP) for decision making by optimizing the time to resolution for emergency and crisis situations		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IOP.008	General Requirements	IOP platform shall provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making		
IOP.009	General Requirements	IOP platform should provide a multi -agency collaboration tool to support instant communication between various user groups and authorities accessing IOP interface		
IOP.010	General Requirements	IOP platform should facilitate training mechanism		
IOP.011	Location Requirements	Platform shall have a GIS based map to provide the location detail		
IOP.012	Location Requirements	Multiple layer maps to be supported as required for various applications		
IOP.013	Location Requirements	GIS maps to comply OGC standards		
IOP.014	Location Requirements	Maps to support Drag & Drop functionality of various sensors at any given point of time		
IOP.015	Location Requirements	Map functionality to provide search options on basis of events, sensors, time etc.,		
IOP.016	Location Requirements	GIS to support addition/removal of sensors/ systems on need based		
IOP.017	Location Requirements	Map to support event based response actions for decision making in case of any emergency / critical situation		
IOP.018	Location Requirements	GIS based application to support Role based authentication for effective management of the system		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IOP.019	Realtime Requirements	CCTV feeds to be viewed on the Map in case of any event triggers , IOP GUI shall also provide the facility to monitor multiple camera feeds in 2X2, 4X4 etc grid views and facilate live view, playback, PTZ control etc.		
IOP.020	Realtime Requirements	System to provide instant threat/event management based on the triggers generated		
IOP.021	Realtime Requirements	System shall provide view and availability of various systems/ sensors on the map at any given time		
IOP.022	Realtime Requirements	System shall facilitate communication between various agencies and personnel to address the situations		
IOP.023	Realtime Requirements	System shall support tracking of real time devices integrated		
IOP.024	Realtime Requirements	System shall trigger alerts for any of the sensors/ applications		
IOP.025	Incident Response	System shall facilitate setting the priority of the event and enable triggering the incidents automatically		
IOP.026	Incident Response	System shall allow setting up multiple triggering rules per incident type		
IOP.027	Incident Response	System shall enable associating response procedures to incident types. The associated procedures should be available for selection to operators upon manual incident creation.		
IOP.028	Post Incident Requirement	Shall have a recording mechanism that includes all the activities such as voice, telephony, Location, triggers etc., including the operator activities for analysis		
IOP.029	Post Incident Requirement	Shall have an event reconstruction functionality to give a complete overview of the synchronous events in the timeframe		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IOP.030	Post Incident Requirement	Shall provide a facility to export all the event scenario as a playable media file		
IOP.031	Post Incident Requirement	System shall support sorting and filtering the list of incidents		
IOP.032	Assets Management	System should present the operator with a logical tree that contains devices from different types		
IOP.033	Assets Management	System shall allow searching the device tree by device name or device type		
IOP.034	Assets Management	System shall indicate the device type by an icon		
IOP.035	Assets Management	System should display a pop-up for a device with its details		
IOP.036	Health Management	System should be able to monitor of both physical servers and system components (e.g. services, plug-ins) including CPU/Memory/Disk utilization and network connectivity performance		
IOP.037	Web Intelligence	System should have a tool for monitoring websites and social networks for topics of interest over time such that it should monitor new information on a variety of requirements from multiple sources in one platform.		

2.11 Data Centre Specification

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DC.001	Data availability	99.982%		
DC.002	Receiving Power	Commercial power		
DC.003	UPS	UPS system with N+N redundancy		
DC.004	Generator	Gen-set with N+1 redundancy		
DC.005	Power Provision	Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement		
DC.006	Cooling Features	BuildingRack base cooling		
DC.007	Fire Protection:	High Sensitive Smoke Detectors, Fire Suppression System		
DC.008	Security	CCTV surveillance cameras, 24x7 on-site security presence, building Access and rack access (Photo ID Card must) along with biometric authentication		

2.12 Core Router

S. No	Minimum Technical Specifications	Compliance (Yes / No)	Deviations / Remarks
CR.001	The Core Router should be chassis based, should have redundant processor and redundant power supply. All the Interfaces should be provided in line cards and no interface should be on CPU card. All interface should have wire speed performance. The back-plane capacity of Router should be minimum 700Gbps & forwarding performance of 1000 Mpps packets per sec of 64 bytes packet. The performance is considered with IPv4 & IPv6.		
CR.002	Interface Requirement: 16 X 1 Gig Base SFP interface and 4 X 10Gig interface (The optics should be populated from day one) and Chassis should have atleast 3 free main slot (not dauther slots) to scale in future to support additional 8 X 10Gig interface or 60 X 1 Gig interface in future.		
CR.003	The Router should have High Availability Features: Non-Stop Routing, Graceful Restart, In Service Software Upgrade, 802.1ag, MC-LAG, BFD for IPv4 and IPv6, VRRP.		
CR.004	Protocol: DHCP, IP Multicast, PIM SM, PIM SSM, IGMP, MLD, RP, Next generation Multicast using MPLS LSP, IS-IS, HQOS, LDP, MPLS, MPLS FRR, L2 VPN, L3 VPN, VPLS, Diff Serv TE, RIP V 2, OSPF, BGP, NAT		
CR.005	Router should have IPv4, IPv6 and QoS Classification. Should have 3M IPv4 and 2M IPv6 routing entries per system. Should have support for 15 logical routers.		
CR.006	Network Management: SNMP v2 and upgradable to SNMP V3, Console management access, NTP or SNTP		
CR.007	Certification: Router should be NEBS certified and EAL 3/NDPP certified under Common Criteria.		

2.13 Core Switch

S.No	Item	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
CS001	Technical Requirement	Redundancy: Atleast 2 Switch Fabrics to support bandwidth for future Highly Scalable Ethernet Standards from Day 1. Should have redundant power supply from day 1.		
CS002	Technical Requirement	Interface support: 40G from Day 1, Support up to 40 Nos of 10 Gigabit Ethernet or 40 Gigabit Ethernet ports		
CS004	Technical Requirement	HA Features: All the main components like power supplies and fans etc should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable. The switch in redundancy shouldbe working in an active-active load sharing mode, Support for Hot Swap of all redundant components: Line Cards, power supply, and fan trays		
CS005	Technical Requirement	Should support 64K MAC table, 4K VLAN and sufficient DRAM to meet smooth operation of switch. Bidders should offer solution to meet the routing requirements of defined applications		
CS006	Technical Requirement	Protocols: IEEE 802.1w RSTP and IEEE 802.1s MSTP, RIP V1/v2, OSPF v1/v2, BGPv4, IPv6 packet switching. VRRP, should support MPLS, GRE tunnelling, IP Multicast PIM - SSM, MSDP, IGMP v1, v2, v3, IGMP Snooping, H/W based IPv4 and IPv6 Multicasting		
CS007	Technical Requirement	Security Features: ACL, DHCP replay, Dynamic Arp, MAC address based filtering, RADIUS, TACACS+		
CS008	Technical Requirement	Monitoring: Should Support SNMP, RMON/RMON-II, SSH, telnet, web management through network management software,		
CS009	Technical Requirement	IEEE Standards: IEEE 802.1AB, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1s, IEEE 802.1w, IEEE 802.3ae, IEEE 802.3ah/IEEE 802.3ag, IEEE 802.3ad,ITU-T G.8032/equivalent open standard for sub 50ms ring protection		

2.14 Internet Firewall

S.No	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
FW.001	The Firewall should have minimum 6 x 10G supporting SFP+ interfaces & 8 x 1G BaseT RJ45 ports to cater to connectivity from multiple service providers and load balance them, Throughput should be 50 Gbps on 64 bype packet size, IPSec Throughput of 10 Gbps, 4000000 new session per second, 50M concurrent session, 5Gbps of SSL VPS throughput, 1000 Site to Site VPN and 1000 SSL VPN, 20 Gbps of IPS Throughput. The firewall should have integrated redundant power supply.		
FW.002	Features: Should support NAT64, DNS64 & DHCPv6, Traffic Shaping, should support Virtualization (Virtual Firewall, Security zones and VLAN). Minimum 10 Virtual Firewall license should be provided and upgradation option up to 100 virtual Firewall should be there for Future expansion, IPv6 IPSec feature to support for secure IPv6 traffic in an IPSec VPN.		
FW.003	The Firewall, IPSEC & SSL VPN modules shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Certification.		
FW.004	Intrusion Prevention System: IPS capability shall minimally attain NSS Certification, ICSA labs certification. 20 Gbps for Enterprise Mix / Real world traffic Throughput. Should able to inspect SSL based traffic. Should have atleast 7,000 Signature.		
FW.005	Threat Prevention: The Firewall should have at least 10 Gbps of Threat prevention throughput on Mix / real world traffic		
FW.006	Web Content Filtering: The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules. should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic. system shall be able to queries a real-time database of over 110 million + rated websites categorized into 70+ unique content categories. Antivirus capability shall be ICSA labs certified.		

S.No	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
FW.007	Application Control: The proposed system shall have the ability to detect, log and take action against network traffic based on over 2500 application signatures		
FW.008	Data Leakage Prevention: The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.		
FW.009	UTM Module & Subscriptions: OEM should have in house development and subscriptions for all UTM Modules including IPS, App Control, Antivirus, Web content filtering.		
FW.010	High Availability: The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component		
FW.011	The device shall support stateful session maintenance in the event of a fail-over to a standby unit. High Availability Configurations should support Active/Active or Active/ Passive		

2.15 DC Firewall

S.No	Technical Specifications for Next Generation Firewall	Compliance (Yes / No)	Deviations / Remarks
DCFW.001	The Firewall appliance should be a purpose-built appliance based solution with integrated functions like Firewall, VPN and User awareness. The product licensing should be device based and not user/IP based (should support unlimited users except for VPN). The hardware platform & Firewall with integrated SSL/IPSec VPN application has to be from the same OEM. The quoted NGFW OEM must have NSS Lab's Recommended rating as per latest NSS Labs NGFW Methodology testing with a minimum exploit blocking rate of 95%.		
DCFW.002	Throughput capacity of firewall under test conditions should not be less than 70 Gbps. Throughput capacity of VPN under test conditions should not be less than 15 Gbps. Appliance should support Max 25,000,000 concurrent sessions. Appliance should support at least 1,80,000 connections per second. Solution should be based on multi core processors and not on proprietary hardware platforms like ASICs, Should have minimum 16 GB memory with option of upgradable up to 32 GB. Hardware should have field upgradable capabilities for upgrading components like network cards, RAM, power supplies, fan etc.		
DCFW.003	Solution should have following deployment modes mandatory: a) L3 Mode, b) L2/Transparent Mode. The solution should be deployed in High Availability. Should support hardware fail open cards for critical interfaces. NGFW appliance should have inbuilt storage of 900 GB SSD / HDD.		
DCFW.004	Interface Requirement: 8 x 10/100/1000 Base-T Copper Ports, 4 x 10 GB 10G SFP ports from day 1 and support for addition of 2 x 40G SFP ports. Dedicated Management and Sync Ports		
DCFW.005	Firewall Feature: solution should be based on "stateful inspection" technology and must support access control for at least 500 predefined /services/protocols with capability to define custom services. Must allow security rules to be enforced within time intervals to be configured with an expiry date/time. The communication between the management servers and the security gateways must be encrypted and authenticated with PKI Certificates.		
DCFW.006	Authentication: schemes must be supported by the security gateway and VPN module: tokens (ie - SecureID), TACACS, RADIUS and digital certificates. Should support Ethernet Bonding functionality for Full Mesh deployment architecture. Must support user, client and session authentication methods.		

S.No	Technical Specifications for Next Generation Firewall	Compliance (Yes / No)	Deviations / Remarks
	User authentication schemes must be supported by the security gateway and VPN module: tokens (ie -SecureID), TACACS, RADIUS and digital certificates. Firewall should support the system authentication with RADIUS and local authentication. Both should work simultaneously. Solution must support DCHP, server and relay. Solution must include the ability to work in Transparent/Bridge mode.		
DCFW.007	Solution must support gateway high availability and load sharing with state synchronization. Solution must support Configuration of dual stack gateway on a bond interface, OR on a sub-interface of a bond interface. Solution must Support 6 to 4 NAT, or 6 to 4 tunnel.		
DCFW.008	User Identity / Awareness: Must be able to acquire user identity from Microsoft Active Directory without any type of agent installed on the domain controllers. Must support Kerberos transparent authentication for single sign on. Must support the use of LDAP nested groups. Must be able to create rules and policies based on identity roles to be used across all security applications. The solution should have the inherent ability to detect multi-stage attacks. For the purpose of detecting multi stage attacks the solution should include static analysis technologies like antivirus, anti-malware/anti bot however in an integrate mode with the solution. The bidder or SI may use additional appliances (at max 2) for the solution but should be provided by the same OEM in the solution.		
DCFW.009	The solution should inspect the web sessions (HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted. The proposed solution should dynamically generate real-time malware intelligence for immediate local protection via integration with the separate Automated Management and Event Correlation System. This Automated Management and Event Correlation solution must be from the same OEM.Solution should have an ability to remove all the active content and macros sending only a clean document to the end user. Solution should be able to detect & Prevent the Bot communication with C&C.		
DCFW.010	Solution should have aMulti-tier engine to ie detect & Prevent Command and Control IP/URL and DNS. Solution should be able to detect & Prevent Unique communication patterns used by BOTs ie Information about Botnet family. Solution should be able to detect & Prevent attack types ie, such as spam sending click fraud or self-distribution, that are associated with Bots. Solution should be able to		

S.No	Technical Specifications for Next Generation Firewall	Compliance (Yes / No)	Deviations / Remarks
	block traffic between infected Host and Remote Operator and not to legitimate destination. Solution should be able to provide with Forensic tools which give details like Infected Users/Device, Malwaretype, Malware action etc		
DCFW.011	Security Management: A separate centralized management appliance/software needs to be provided for management and logging of NGFW appliance. In case other security components like APT solution etc. are from the same OEM then a single centralized management, logging (and not multiple management system) should manage all such security devices. Security management Hardware can be an OEM appliance or dedicated server with software. In case of dedicated server, Server should be rack mounted with Intel based 8 core processor with min two nos. of 64-bit processor having 64 GB RAM or OEM recommended whichever is higher for these specifications. Minimum 2 TB Hard disk and minimum dual 10/100/1000 Mbps network port. The central management console and should be able to handle 5000 log/sec.		
DCFW.012	Security management application must support role based administrator accounts. Management must provide functionality to automatically save current state of Policy each time when any configuration changes in Security policy is enforced, and should have option to revert back to previous state stored state. It must be capable of storing at least last 5 policies. Management Solution must include a Certificate-based encrypted secure communications channel among all vendor distributed components belonging to a single management domain. The management must provide a security rule hit counter in the security policy. Solution must include a search option to be able to easily query which network object contain a specific IP or part of it. Solution must have a security policy verification mechanism prior to policy installation.		
DCFW.013	The Log Viewer should have the ability view all of the security logs of all functions managed by the solution in one view pane (helpful when troubleshooting connectivity problem for one IP address)		
DCFW.014	The Log Viewer should have the ability in the log viewer to create filter using the predefined objects (hosts, network, groups, users...)		

2.16 WAN Internet Router

S. No	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
IR.001	The router should be modular in architecture with minimum 3 slots and should be a single chassis solution, should support redundant Router processors / Routing engines and Redundant Power supply. All modules, fan trays & Power supplies should be hot swappable.		
IR.002	Router Should have minimum 35 Gbps throughput from day 1 with minimum 50 Mpps with services on IPv4 and IPv6. Route Processors should have minimum 4GB of flash memory, 4GB of RAM/DRAM		
IR.003	Minimum 6 x Gigabit Ethernet routing ports with copper transceivers and 4x Gigabit Ethernet Ports (Supporting long haul and short haul SFP). hold support wide variety of interfaces including 10G, OC3, OC48, DS3, ChE1/T1 WAN interfaces, should support 4 x 10G ports.		
IR.004	Features: QoS classification, policing and shaping, NAPT44, NAPT64, NAT-PT, NAPT66,NAT44, 6to4, Twice-NAT44, 6in4, PAT-PP, Dynamic-NAT, ACL, Router should support hardware encryption capabilities.		
IR.005	Should support 250k IPv4 and 250k IPv6 Routes, 200k MAC addresses, 1000 VRFs		
IR.006	Protocols: Should support RIPv2, OSPF, IS-1S and BGP4, LDP, BFP routing protocols & IP multicast routing protocols: PIM , IGMP , MPLS, PWE3, FRR, VPLS, NAT, PAT, RADIUS, TACACS+,		
IR.007	Security Features: should support IPv6 for IPSec encryption for data confidentiality, 3DES and AES encryption standards		
IR.008	Management: SNMP V1 and V2, Telnet, TFTP		
IR.009	certification: EAL3/ NDPP or above Certified		

2.17 Distribution Switch

S.No.	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
DSW.001	The Should have Non-blocking (WireSpeed) Architecture with Minimum 24 ports of 10/100/1000 base-T and 4 SFP+ uplink ports (populated with required modules). 1 U Rack mountable and should provide stacking of minimum 9 switches with 80 Gbps of dedicated stacking bandwidth (All required accessories, licenses to be provided). Switch should support internal redundant power supply.		
DSW.002	128 Gbps or higher Backplane capacity and minimum 90 Mpps of forwarding rate, Support for at least 4000 VLANs & 16k MAC address		
DSW.003	Protocol: IGMP snooping v1 & v2, static IP routing and RIP from day 1, Should be upgradable to OSPF, OSPFv3, RIPnG, PIM, MLD in future, SSH, SNMPv3, DHCP,		
DSW.004	Management : Switch needs to have console port for administration & management, Management using CLI, GUI using Web interface should be supported, FTP/TFTP for upgrading the operating System, SNMP v1,v2,v3, Switch should be manageable through both IPv4 & IPv6.		
DSW.005	IEEE Standards: IEEE 802.1x, IEEE 802.1D, IEEE 802.1p, class-of-service, IEEE 802.1Q, IEEE 802.3 10BASE-T, IEEE 802.3u 100BASE-TX		
DSW.006	Switch should be FCC Part 15, ICES-003, VCCI Class A, EN 55022, EN 55024, EN 300386, CAN/CSA 22.2 No.60950-1, IEC60950-1, Reduction of Hazardous Substances (ROHS) 6 certified		
DSW.007	Should have modular OS and should support configuration roll back to recover mis-configured switch to last known good configuration		

2.18 Blade Chassis

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
BCH.001	Blade Chassis	Blade chassis shall be 19" standard Width rack mountable and provide appropriate rack mount kit.		
BCH.002	Blade Chassis	The power supply modules should be hot pluggable		
BCH.003	Blade Chassis (Redundancy)	The power subsystem should support all of the following modes of power redundancy (No redundancy, N+1 , N+N or grid)		
BCH.004	Blade Chassis (Redundancy)	The power subsystem should be support N + N power redundancy for a fully populated chassis with the 2 socket (CPU) servers		
BCH.005	Blade Chassis (Redundancy)	Should be configured to provide full redundant cooling to all blade slots		
BCH.006	Fibre Channel Interconnects	The uplink from the chassis should support FCoE (Fibre Channel over Ethernet) technology		
BCH.007	Management	Support remote KVM / virtual KVM capability for management and administration.		
BCH.008	Blade Chassis (DVD)	Support virtual DVD and virtual floppy internally / externally		
BCH.009	Interface	Fabric switches should support the direct connection to FCoE enabled storage arrays		
BCH.010	Management	Support a stateless environment where server identity is created by the administrator who defines the server		
BCH.011	Blade Chassis	Servers can be automatically assigned to the resource pools based on qualification criteria		
BCH.012	Management	Support the ability to rollback firmware from current active versions to the previous version for the Server BIOS, Adapter firmware and boot code versions, individual		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		server management chips from the same console		
BCH.013	Management	Role Based Access Control so that the resources can be managed by respective resource administrator.		
BCH.014	Server Management	Movement of server identity from one slot to another in the event of server failure		
BCH.015	Power Management	Administrators have the flexibility to define power policies so that the power can be limited to a specific server		
BCH.016	Power Management	Administrators should be able to decide the threshold / cap on the maximum power that the chassis can draw.		
BCH.017	Server Management	Supports multiple level of authentication methods such as RADIUS / TACACs+ and LDAP		
BCH.018	Server Management	Movement of server identity from one slot to another in the event of server failure		
BCH.019	Support	System should not be an end of life / end of service product.		

2.19 Servers

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SERV.001	Processor	Latest series/ generation of 64bit x 86 processor(s) with ten or higher Cores. Processor speed should be minimum 2.4 GHz Minimum 2 processors of 16 core each per each physical server		
SERV.002	RAM	Minimum 128 GB Memory per physical server		
SERV.003	Internal Storage	2 hot swap disk SSD with extensible bays		
SERV.004	Network interface	2 X 20GbE LAN/WAN ports for providing Ethernet connectivity Optional: 1 X Dual-port 16Gbps FC HBA for providing FC connectivity MSI can determine their own architecture for non-blocking network infrastructure.		
SERV.005	Power supply	Redundant chassisPower Supply		
SERV.006	RAID support	As per requirement/solution		
SERV.008	Form Factor	Rack mountable/ Blade		
SERV.009	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE and Citrix or any other industry standard product as designed by MSI.		

2.20 External Storage - SAN/NAS/ Unified storage

S. No	Item	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
STO.001	Connecting Ports (SAN)	Should have minimum of 2 * 10 Gbps iSCSI and 2 16 Gbps FC Ports per Controllers.		
STO.002	Management Software	Must include Storage Manager software, to centrally manage all Storage subsystems, Multi-path (Load Balancing & Failover), LUN masking and should Support RAID migration on to the vacant space available		
STO.003	O/S Support	Support for multiple Operating Systems connecting to it, including of Windows, UNIX, Linux, AIX, HP UX etc.		
STO.004	Disk Capacity	Offered SAN Array shall be configured with 1250 TB usable capacity in RAID 6 using NL SAS drives.		
STO.005	Raid Controllers	Dual, both Active, Minimum 96 usable cache across Controllers (Min 32 GB per Controller).		
STO.006	Protocol support	FC, iSCSI/ NFS/CIFS/FCoE		
STO.007	Cache safety	Cache should be mirrored and battery-backed-up /disk-de-staged, to provide protection of data for 72 hours or more.		
STO.008	Drive Interface	12 Gbps SAS /4 Gbps FC-AL, with auto-sensing,		
STO.009	Supported drives, Mixed drive	Should support SSD, SAS,NL-SAS, 12 GBPs Drives.		
STO.010	RAID Levels	0/1, 4/ 5, and 6 or equivalent		

S. No	Item	Minimum Technical Specification	Compliance (Yes / No)	Deviations / Remarks
STO.011	Min. Usable capacity support	The system should be scalable to minimum 2.0 PB Usable capacity in RAID 6 using NL SAS drives.		
STO.012	Fans & Power Supplies	Minimum 2, Dual-Power, redundant, hot-swap Power supplies for storage and switches		
STO.013	Rack Support	Suitable for industry-standard Racks and PDUs		
STO.014	Data Services	Should include data Snapshot, Thin provisioning, Volume cloning or equivalent features for the offered capacity of the storage array. The proposed system should also include storage based replication software (Any Hardware if required needs to be provided).		
STO.015	Reconfiguration	storage should support RAID /LUN migration.		
STO.016	Warranty & Support	3 Years, Comprehensive, On-Site Support Warranty including part replacement /repairs within 8 hours of reporting, and Software support for updates, upgrades, patches, and bug fixes for supplied s/w from OEM 24 x 7 x 365 days.		
STO.017	Alerts	Automated alerts for Improving service response times.		
STO.018	Others	All required cable and connectors to be supplied		

2.21 Virtualization Software

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VIRSO.001	Solution	Sits directly on the server hardware with no dependence on a general-purpose OS for greater reliability and security.		
VIRSO.002	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.		
VIRSO.003	VM Capability	Create Virtual machines with up to 128 virtual processors, 6 TB virtual RAM and 2GB Video memory in virtual machines for all the guest operating system supported by the hypervisor. The MSI can propose a more optimum solution that suggested above.		
VIRSO.004	VM Live Migration	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and between servers in a cluster, across clusters as well as long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.		
VIRSO.005	Storage Live Migration	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.		
VIRSO.006	High Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.		
VIRSO.007	Always Available	Zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.		
VIRSO.008	Resource Addition	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.		
VIRSO.009	Resource Scheduler	Dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		physical hosts. 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.		
VIRSO.010	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and in-motion and also provides 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 Firewall and HIPS solutions without the need for agents inside the virtual machines from day 1.		
VIRSO.011	Storage support	Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integrate with NAS, FC, FCoE and iSCSI SAN and infrastructure from leading vendors leveraging high performance shared storage to centralize virtual machine file storage for greater manageability, flexibility and availability. Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.		
VIRSO.012	OEM Support	Direct OEM 24x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.		
VIRSO.013	Virtual Switch	Span across a virtual datacentre and multiple hosts should be able to connect to it. This will 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 will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details. "Latency Sensitivity" setting in a VM that can be tuned to help reduce virtual machine latency. Link aggregation feature in the virtual switch which will provide choice in hashing algorithms on which link aggregation in decided and this should also provide multiple link aggregation groups to be provided in a single host.		
VIRSO.014	VM based Replication	Efficient array-agnostic replication of virtual machine data over the LAN/WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.		
VIRSO.015	VM Backup	Simple and cost-effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability.		
VIRSO.016	I/O Control	Prioritize storage access by continuously monitoring I/O load of storage volume and dynamically allocate available I/O resources to virtual machines according to needs. Prioritize network access by continuously monitoring I/O load over network and dynamically allocate available I/O resources to virtual machines according to needs.		

2.22 TOR (Top of the Rack) Switch

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
TORS.001	Ports	▪ 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra 2 numbers of Uplink ports (40GE) ▪ All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports. ▪ MSI can propose a non-blocking architecture		
TORS.002	Switch type	Layer 3		
TORS.003	MAC	Support 32K MAC address.		
TORS.004	Backplane	Capable of providing wire-speed switching		
TORS.005	Throughput	500 Mbps or better		
TORS.006	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
TORS.007	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
TORS.008	Protocols	▪ IPV4, IPV6 ▪ Support 802.1D, 802.1S, 802.1w, Rate limiting ▪ Support 802.1X Security standards ▪ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ▪ 802.1p Priority Queues, port mirroring, DiffServ ▪ DHCP support ▪ Support up to 1024 VLANs ▪ Support IGMP Snooping and IGMP Querying ▪ Support Multicasting ▪ Should support Loop protection and Loop detection,		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		▪ Should support Ring protection		
TORS.009	Access Control	▪ Support port security ▪ Support 802.1x (Port based network access control). ▪ Support for MAC filtering. ▪ Should support TACACS+ and RADIUS authentication		
TORS.010	VLAN	▪ Support 802.1Q Tagged VLAN, port based VLANs and Private VLAN ▪ Switch must support dynamic VLAN Registration or equivalent ▪ Dynamic Trunking protocol or equivalent		
TORS.011	Protocol and Traffic	▪ Network Time Protocol or equivalent Simple Network Time Protocol support ▪ Switch should support traffic segmentation ▪ Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number		
TORS.012	Management	▪ Switch needs to have a console port for management via a console terminal or PC ▪ Must have support SNMP V1, V2 and V3 ▪ Should support 4 groups of RMON ▪ Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface		
TORS.013	Resiliency	▪ Dual load sharing AC and DC power supplies ▪ Redundant variable-speed fans		

2.23 APT (advanced persistent threat protection)

Sr No	Minimum Specifications for APT Solution	Compliance (Yes / No)	Deviations / Remarks
APT.001	The APT appliance should be a purpose built on premise appliance based solution with integrated support for sandboxing. Cloud based solution will not be accepted.		
APT.002	The hardware based solution should provide protection for all incoming and outgoing web and email traffic from /to Internet.		
APT.003	The quoted APT OEM must have NSS Lab's Recommended rating as per breach detection system methodology2.0 and should have block rate of at least 95%		
APT.004	The APT appliance should be able to handle min 2 Gbps incoming /outgoing traffic (throughput) and for at least 10,000 users.		
APT.005	The APT appliance should be able to process min 1,000,000 files/month (either web or mail or both)		
APT.006	Appliance should have minimum 2 x 1 TB storage in RAID 1.		
APT.007	The APT appliance should support at least 36 virtual machines running simultaneously		
APT.008	Min 4 Copper and 2 x 10G Fibre ports should be provided in APT appliances for achieving functionalities mentioned		
APT.009	Minimum one number of 1G Copper ports for management.		
APT.010	The Hypervisor used by sandboxing solution must not be an OEM solution such as from VMWare, HyperV, VirtualBox, RHEV etc however it should be a custom Hypervisor purpose built for sandboxing requirement		

Sr No	Minimum Specifications for APT Solution	Compliance (Yes / No)	Deviations / Remarks
APT.011	The solution must be able to detect and report malware by using multiple images of Windows XP, 7, 8 and 10 etc.		
APT.012	The solution must support prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licences for sandboxing solution		
APT.013	Anti-APT solution should be able to work independently of signature updates from OEM website.		
APT.014	The solution must be able to support scanning links inside emails/documents for zero days & unknown malware and support sandboxing of file sizes between 2 Kb and 50 MB. Solution should have an ability to remove all the active content, harmful links in email message/documents and macros sending only a clean document to the end user		
APT.015	The solution should inspect the web sessions(HTTP and HTTPS both) to detect and notify the malicious web activity including malicious file downloads through the internet. Third Party/Separate appliance for SSL offloading will not be accepted		
APT.016	The solution to be provided with complete endpoint detection and response (EDR) solution for at least 1000 endpoints and should work seamlessly with the same.		

2.24 Centralized EDR

S. No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
EDR.001	The offered solution should perform the following min tasks at endpoints:		
	a. Endpoint Firewall		
	b. Endpoint Application Control		
	c. Media Encryption on HDD and USB		
	d. Prevention of C&C and BOT traffic directly at endpoint		
	e. Anti Ransomware Features		
	f. Anti Phishing Protection		
	g. Compliance Monitoring capabilities		
	h. Endpoint Level Forensics		
EDR.002	The offered solution must be from the same OEM as that of the APT and should integrate with the sandboxing device installed under APT solution. In case EDR and APT solution are from different OEM then an on-premise sandboxing solution must be providing with the EDR solution. Solution must include a Zero-hour protection mechanism for new viruses, malwares spread through email and spam without relying solely in heuristic or content inspection. Ableto perform different scan Actions based on the virus type or abnormal behaviour observed (Trojan/ Worm, Hoax, Virus, other)		
EDR.003	Solution must have capabilities to isolate and quarantine the endpoints from the network in scenarios where windows patches, hotfixes, services packs, virus definitions are missing or outdated on the endpoint. The solution must have capabilities to prevent against all families of ransomwares and restore encrypted files in event of a ransomware attack.		
EDR.004	The solution must have capabilities to prevent users from accessing phishing websites and URLS and prevent the users from entering corporate credentials on phishing websites. Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.		

S. No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
EDR.005	The solution must support multiple remote installations. Shall provide for notification options for Virus, malwares, advanced threats, URLs, C&C call-backsetc. Shouldbe capable of providing multiple layers of defence from Known as well as unknown threats like zero days, worms, malwares, APT attacks at endpoint		
EDR.006	Shall have facility to clean, delete and quarantine and restore the virus, malware, and ransomware affected files. Should support scanning for ZIP, RAR compressed files, and TAR archive files. Should support online update, where by most product updates and patches can be performed without affecting the normal operations. Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks).		
EDR.007	Should support memory scanning at the endpoint and advanced threat analysis to a centralized sandboxing device on the network from the endpoints. Updates to the scan engines should be automated and should not require manual intervention.		
EDR.008	All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security. Updates should be capable of being rolled back in case required		
EDR.009	Should support various types of reporting formats such as CSV, HTML and text files. Should provide native forensics capabilities for the endpoints and should be able to perform forensics even when outside the network perimeter or in offline mode.		
EDR.010	Should provide in browser protection through plugin or add on mechanism to prevent and control download of malicious and unknown attacks and by blocking access to data entering on phishing websites, by removal of harmful active content in files and by converting potentially harmful files to PDF.		
EDR.011	Should integrate with the sandboxing solution provided in APT solution. The solution must be provided with a centralized management console to manage at least 500 endpoints.		

2.25 SIEM for Logs & Packets System

S. No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
SIEM.001	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network visibility through deep packet inspection high speed packet capture and analysis.		
SIEM.002	SIEM for Logs and deep packet inspection should be from same OEM.		
SIEM.003	The solution should be a physical appliance form factor with following components:		
	a. Management & Reporting		
	b. Normalization and Indexing		
	c. Correlation Engine		
	d. Data Management		
SIEM.004	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.		
SIEM.005	The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP, and Encryption.		
SIEM.006	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.		
SIEM.007	Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information		

S. No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	asset like IP/Device etc		
SIEM.008	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.		
SIEM.009	A single log appliance should support minimum 30,000 EPS and packet appliance should support up to 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.		
SIEM.010	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 100,000 EPS.		
SIEM.011	The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. Solution should be sized to provide online storage for 1 year at central site. Both raw logs and normalized logs should be made available with minimum 90 TB of storage provided by OEM		
SIEM.012	The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize it’s response to help ensure effective incident handling.		
SIEM.013	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required		
SIEM.014	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.		
SIEM.015	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration		
SIEM.016	Should store RAW packet DATA for 7 days and normalized packet data for 30 days for forensics.		
SIEM.017	Should be able to provide complete packet-by-packet details pertaining to one or more		

S. No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.		
SIEM.018	Should be able to filter the captured packets based on layer-2 to layer-7 header information.		
SIEM.019	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.		
SIEM.020	The proposed solution must be able to provide the complete platform to perform Network forensics solution		
SIEM.021	The solution must be able to detect malicious payload in network traffic		
SIEM.022	· Detect and reconstruct files back to its original type		
SIEM.023	· Detect hidden or embedded files		
SIEM.024	· Detect and flag out renamed files		
SIEM.025	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure.		

2.26 Application Delivery Controller

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	Architecture		
ADC.001	Should be high performance purpose built next generation multi-tenant hardware with multicore CPU support. Platform should support multiple network functions including application load balancing, application firewall, SSL VPN & global server load balancing functions with dedicated hardware resources for each virtual instance. Platform should have option to support 3rd party network functions		
ADC.002	The appliance should have minimum 8 x10G SFP+ data interfaces from day one, The appliance should support Minimum 32GB RAM and 2*SSL ASICS/FGPA/cards with network virtual function support		
ADC.003	Next generation multi-tenant platform must support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each network function must have assigned dedicated hardware resources including I/O interfaces, memory, CPU, SSL card in order to ensure every network functions performs without affecting other functions		
ADC.004	Platform should support at least 2 network functions in order to cater current and future requirements and performance numbers including throughput, connections, SSL throughput and SSL transactions must be per virtual instance.		
ADC.005	For Load balancer – network function : 1. Load balancer network function with minimum 18 Gbps of system throughput , 2. Minimum of 1200K concurrent connection per virtual instance , 3. Minimum of 9000 SSL transaction Per Second per instance, 4. Dedicated Management Interface.		
ADC.006	For Web Application Firewall – network function : 5. There should be dedicated instance for Web Application Firewall with at least 1Gbps of layer7 throughput.		
ADC.007	Scalability : Platform should have additional capacity to accommodate at least 1 additional WAF function with 100bps of throughput or 2 additional load balancer virtual functions of similar		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	capacity or 4 additional load balancer virtual function of half capacity mentioned above with license upgrade		
ADC.008	Application Load balancing – Network Function		
ADC.009	Should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing support, The appliance should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, snmp, SIP session ID, hash header etc. Support for policy nesting at layer7 and layer4, solution should able to combine layer4 and layer7 policies to address the complex application integration.		
ADC.010	Script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. Load balancer should support ePolicies to customize new features in addition to existing feature/functions of load balancer. Traffic load balancing using ePolicies should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash ip and snmp.		
ADC.011	Should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.. Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.		
ADC.012	should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers. Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..		
ADC.013	Should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048 and 4096 bit keys for encrypted application access.		
	Global Server Load balancing – network Function		
ADC.014	The Proposed Solution Should be act as a SDNS(Smart DNS). The appliance should support global server load balancing algorithms including weighted round robin, geographic, global least		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	connections, global connection overflow, ip overflow, static proximity, dynamic proximity.		
ADC.015	Solution should also support full DNS server to support all kind of DNS records including A, AAAA, MX, CNAME, PTR DNS records with option to import zone file on the device. Should support dynamic proximity rules instead of static proximity rules to direct the traffic to closest datacentre		
ADC.016	The Proposed Solution should Support of DNS Sec. The Proposed Solution should support multiple health check like ICMP, TCP http and https under GSLB module.GSLB should be deployable without any dependencies like placement of solution. (E.G whether device placed in GSLB or perimeter level GSLB should work).		
	Web Application Firewall – network function		
ADC.017	The Web application firewall virtual function should support positive security model with machine learning capabilities to detect and prevent anomaly in application traffic and unknown attacks. Machine learning should be based on true ML algorithms, and not just automation of dynamically learnt rules. Positive security model should be fully automated without requiring human assistance to learn and deploy rules. In other words system should be auto configurable without requiring any human actions "Learning phase", "Tuning Phase" and then "production phase".		
ADC.018	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. WAF positive security model should be intelligent to adapt changes to existing modules of application or dynamically handle new modules without any manual learning and fine-tuning		
ADC.019	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), nonstandard encoding and Session Management. The Web application firewall should address unknown attacks based on user inputs and application responses using combination of dedicated protectors/signature engines and Machine Learning		
ADC.020	WAF should support built-in correlation engine to detect atomic attacks and complex attack chains. Administrator should have option to define customized correlation rules		
ADC.021	□ Administrator should have option to define customized correlation rules, edit and create		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	new correlation rules		
ADC.022	WAF correlation should also identify complex attack chains, and not just aggregate events based on attacks or sources.		
ADC.023	Correlation should not be just an aggregation of multiple events, but detail the classification, prioritization and aggregation		
ADC.024	Should protect web application against layer7 DDOS attacks such as HTTP GET-flooding HTTP Proxy flooding etc. WAF should performs continuous behaviour profiling using machine learning algorithms, continuously dealing with all incoming HTTP requests and application health status and notify security administrator about upcoming DDOS attacks		
ADC.025	WAF should provide advanced bot detection mechanism based on smart combination of signature-based and heuristic analysis. Integration with third party solutions such as antiviruses, DLP, anti-DDoS, firewalls etc. to provide advanced multi-layer protection.		
ADC.026	WAF should be able to provide retrospective analysis of web application attacks either by consuming relevant log files or PCAP files. WAF should provide, content rich graphical user interface, based on web UI, and should be able to renter information as per WAF Admin’s requirements, right from switching to simple / advanced view, to multi-level grouping of attacks. WAF should be able to filter dashboard events using any of the parameters like, time of event, event message, application parameter in question, tags, geo locations, source IP’s, various browser level information, correlation id, policy ID, etc. WAF should provide, client side analytics, including information monitoring sessions (e.g. token tracking), client side intelligence e.g. application being rendered or not, or whether the requester is a bot or not.		
	Clustering and failover		
ADC.027	Should provide comprehensive and reliable support for high availability both at device level and Virtual function level		
ADC.028	Device level HA should support synchronization of network functions configuration from primary/master device to secondary/slave device		
ADC.029	ADC virtual function should support built in failover decision/health check conditions (both hardware and software based) including CPU overheated, SSL card, port health, CPU utilization,		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations / Remarks
	system memory, process health check and gateway health check to support the failover in complex application environment		
ADC.030	ADC VF Should have option to define customized rules for gateway health check - administrator should able to define a rule to inspect the status of the link between the unit and a gateway		
ADC.031	ADC VF Support for automated configuration synchronization support at boot time and during run time to keep consistence configuration on both units.		
	Management		
ADC.032	The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting. The appliance should provide detailed logs and graphs for real time and time basedstatistics. Should capture, log and display traffic related data to analyse for security incidents. Should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should have extensive report and logging with inbuilt tcpdump like tool and log collecting functionality. Should be able to send security incidents via syslog		

2.27 Data Leakage Prevention and Email Security

S.N.	Data Leakage Prevention (DLP)Specifications	Compliance (Yes / No)	Deviations / Remarks
DLP.001	The solution should be able to enforce policies by URL's, domains or URL categories either natively with a Web Security solution. The solution should be able to prevent content getting posted or uploaded to specific geo-destinations on HTTP and HTTPS . The solution should be able to monitor FTP traffic including fully correlating transferred file data with control information and should be able to monitor IM traffic even if its tunnelled over HTTP protocol		
DLP.002	The end point solution should inspect data leaks over HTTP , HTTPs and SMTP. The solution should monitor and control sensitive emails downloaded to mobile devices through ActiveSync. The solution should be able to block outbound emails sent via SMTP if its violates the policy. The proposed solution should work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.		
DLP.003	The endpoint solution should have pre-defined applications and application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture. The endpoint solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network.		
DLP.004	The endpoint would be able to store both structured and unstructured fingerprints on the endpoint itself and should perform all analysis locally and not contact network components to reduce WAN overheads. The solution should be able to enforce different policies for desktops and laptops. The endpoint solution should have capabilities to monitor applications and ensure unauthorized applications do not have access to sensitive files. The endpoint solution should be able to perform discovery only when the endpoint is connected to external power.		
DLP.005	The endpoint solution should encrypt information copied to removable media. The endpoint solution should Blocking of non-Windows CD/DVD burners, it should also Inspect and optionally block Explorer writes to WPD class devices. Endpoint solution should support win 32 and 64 bit OS, Mac &		

S.N.	Data Leakage Prevention (DLP)Specifications	Compliance (Yes / No)	Deviations / Remarks
	Linux OS,Support wide variety of platforms. The proposed solution should be able to encrypt content copied to removable media natively		
DLP.006	The solution should have a comprehensive list of pre-defined policies and templates with over 1700+ patterns to identify and classify information pertaining to different industry like Energy, Petroleum industry vertical etc and India IT Act.		
DLP.007	The proposed solution should provide pre-defined policies for identifying possible for identifying possible expression that are indicative of cyber bullying , self destructive pattern or employee discontent. The solution should be able to detect encrypted and password protected files. The solution should be able to do full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted files or folders		
DLP.008	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives. The solution should be able to enforce policies to detect data leaks even on image files through OCR technology. The solution should enforce policies to detect low and slow data leaks		
DLP.009	The solution should be able to alert and notify sender, sender's manager and the policy owner whenever there is a policy violation, Different notification templates for different audience should be possible. The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI		
DLP.010	The incident should display the complete identity of the sender(Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels. The solution should also allow assigning of incidents to a specific incident manager. The solution should provide automatic notification to incident managers when a new incident is assigned to them and the incident should not allowed for deletion even by the product administrator. The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.		
DLP.011	he solution should support capability called incident risk ranking. It uses statistical data modelling and behavioural baselines to automatically identify and rank groups of high-risk incidents		
DLP.012	The solution must be present in the latest Gartner's leader quadrant for Data Loss Prevention. The		

S.N.	Data Leakage Prevention (DLP)Specifications	Compliance (Yes / No)	Deviations / Remarks
	OEM should have own TAC centre in India.		
	Email security Specifications		
DLP.013	The proposed system should be a dedicated appliance based solution or Virtual Application image for email security. The Solution should have feature of virus scanning engine strip the infected attachments and the Solution should detect known or suspect secure-risk URLs embedded in the email, which are reliable indicators of spyware, malware or phishing attacks.		
DLP.014	The Solution should have feature of virus scanning engine strip the infected attachments and The Solution should detect known or suspect secure-risk URLs embedded in the email, which are reliable indicators of spyware, malware or phishing attacks. The solution should support dictionaries scanning and dictionaries are built-in the product and allow customer to create his own dictionary. The solution should have at least 1500+ predefined content rules inbuilt with Email Security & embedded in the product		
DLP.015	The Solution should have close to 100% virus detection rate for known viruses. The Solution should have multiple AV engines for anti-virus and malware scanning. The Solution should provide proactive virus detection methods for new email-borne virus. The Solution should have feature of virus scanning engine strip the infected attachments.		
DLP.016	The Solution should support URL classification of the embedded links and it contributes for SPAM detection. The solution should support image based spam detection capability, such as the pornography images within the email and it allow customer to adjust the sensitivity level.		
DLP.017	The solution should perform image based filtering. It's should use sophisticated analytical algorithm to analyse image to determine attributes that indicate the image may be of a pornographic or non-pornographic nature in known and unknown spams emails. The solution should have capability to analyse text inside image going through email. The solution should monitor and control sensitive email download to mobile devices through active sync		
DLP.018	The solution should provide the capability of connection control and message rates control for inbound and outbound respectively. The solution should support policy based TLS encryption between mail domains. The solution should have directory harvesting and DoS prevention capabilities. The solution should support internal sender authentication. The solution should provide		

S.N.	Data Leakage Prevention (DLP)Specifications	Compliance (Yes / No)	Deviations / Remarks
	real time IP reputation system. The solution should allow the administrator to specify the re-try time for a delivery failure.		
DLP.019	The solution should have centralized management, including policy configuration, quarantines and logs/reporting. The solution should support the real-time graphical and chart-based dashboard for the summary of email filtering activities. The solution should be able to manage the complete solution - DLP, Email and web security through same centralized management		
DLP.020	The Solution should have option for end user notification for email quarantining letter to be customized and click boxes that enable the user to release e-mail, report false positives, add senders to allow-or block lists and direct links to personal email management portal. The solution should allow where Administrator can specify which queues can be accessed by end user		
DLP.021	The solution should have True Source IP Detection and Connection Blocking feature should work even if Email Security is deployed behind Corporate Email Relay Server/Firewall SMTP. The solution should able to provide the complete forensics of the sensitive outbound data based on the policy defined and should be able to quarantine and release as per automated workflow		
DLP.022	The solution must be from same OEM for optimum operation and manageability and the OEM should have own TAC centre in India.		
DLP.023	The solution should support Domain-based Message Authentication, Reporting, and Conformance (DMARC) validation integration. It should also support Domain Keys (DKIM) Identified Mail integration		
DLP.024	S/MIME encryption		
DLP.025	Anti-Spam / Content Level Detection : The propose system shall minimally integrated following spam detection technologies with unlimited users license for Inbound and Outbound Email Filtering, Extensive Heuristic Spam Filters, Dynamic Heuristic Rule Updates, Attachment Content filtering, Deep Email Header Inspection, Spam Image Analysis Scanning, PDF Scanning / PDF Image Scanning, Global and User Customized Black/White List Filtering, 3rd Party RBL and DNSBL support & Forged IP Checking		
DLP.026	AntiVirus/Spyware Protection: The proposed system should have integrated Antivirus with unlimited users license and provides the following services:		
DLP.027	AV engine and signatures, including legacy virus detection, Automatic update of antivirus and attack		

S.N.	Data Leakage Prevention (DLP)Specifications	Compliance (Yes / No)	Deviations / Remarks
	signatures global network - Push, Scheduled & Manual update, SMTP Messages Virus Scanning, Compressed Attachment and Nested Archive Support, Quarantine Infected files, Replacement Message Notification, Block by File Type, Attachment Filtering		
	AntiMalware Protection		
DLP.028	The solution should combine multiple static with dynamic technologies including signature, heuristic and behavioural techniques.		
DLP.029	The solution should provide virus outbreak prevention through on premise sandboxing solution to protect against a wide range of constantly evolving threats such as ransomware and targeted attacks		

2.28 Intrusion Detection & Prevention System

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
IDPS.001	Performance	Should have an aggregate throughput of no less than 200 mbps Total Simultaneous Sessions – 500,000		
IDPS.002	Features	IDPS should have Dual Power Supply IDPS system should be transparent to network, not default gateway to Network IDPS system should have Separate interface for secure management IDPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.		
IDPS.003	Real Time Protection	Web Protection/ Mail Server Protection Cross Site Scripting SNMP Vulnerability Worms and Viruses/ Backdoor and Trojans Brute Force Protection SQL Injection		
IDPS.004	State full Operation	▪ TCP Reassembly ▪ IP Defragmentation ▪ Bi-directional Inspection ▪ Forensic Data Collection ▪ Access Lists		
IDPS.005	Signature Detection	▪ Should have provision for real time updates of signatures, IPS		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		▪ Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures		
IDPS.006	Block attacks in real time	▪ Drop Attack Packets ▪ Reset Connections ▪ Packet Logging ▪ Action per Attack		
IDPS.007	Alerts	▪ Alerting SNMP ▪ Log File ▪ Syslog ▪ E-mail		
IDPS.008	Management	▪ SNMP v1, v2, v3 ▪ HTTP, HTTPS ▪ SSHv2, Console		
IDPS.009	Security Maintenance	▪ IDPS Should support 24/7 Security Update Service ▪ IDPS Should support Real Time signature update ▪ IDPS Should support provision to add static own attack signatures ▪ System should show real-time and History reports of Bandwidth ▪ IDPS should have provision for external bypass Switch		

2.29 SAN Switch

S. No	Minimum Technical Specifications	Compliance (Yes / No)	Deviations / Remarks
SAN.001	The switch should have non-blocking architecture with 48 ports in a single domain concurrently active at 16 Gbit/sec full duplex with no oversubscription.		
SAN.002	The switch should be configured with base 24 port and can be upgraded to 48 port with PODs		
SAN.003	The switch should support auto-sensing 16,8,4 &2 Gbit/sec FC capabilities. It should also support 10G FC for connecting to WDM devices		
SAN.004	The switch shall support different port types such as F_Port, M_Port (Mirror Port), EX port and E_Port; self-discovery based on switch type (U_Port) and D (Diagnostic Port)		
SAN.005	The switch should be rack mountable.		
SAN.006	Non-disruptive Microcode/ firmware Upgrades and hot code activation.		
SAN.007	The switch shall provide a minimum Aggregate bandwidth of 768 Gbit/sec: 48 ports × 16 Gbit/sec (data rate) end to end.		
SAN.008	Should support Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expeditehigh priority traffic.		
SAN.00	The Switch should be configured with the Zoning and ISL Licenses		
SAN.010	Support for web based management and should also support CLI.		
SAN.011	The switch shall support advanced zoning and ACL to simplify administration and significantly increase control over data access.		
SAN.012	Switch shall support POST and online/offline diagnostics, including RAStrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Path info (FC traceroute), port mirroring (SPAN port).		
SAN.013	Should provide redundant and hot pluggable components.		
SAN.014	The switch should be upgradable to run at 16 Gbit/sec speed by only upgrading SFPs.		
SAN.015	The switch should support automation that simplifies policy based monitoring and alerting		
SAN.016	The switch should support cable and optic diagnostics that simplify the deployment and support of large fabrics		

S. No	Minimum Technical Specifications	Compliance (Yes / No)	Deviations / Remarks
SAN.017	The switch should support 10G FC for DWDM connections		
SAN.018	The switch should support DC power supply as per requirement		
SAN.019	The switch should support 128Gbps Hardware Frame based Trunking		
SAN.020	The switch should support FC, FCR and FICON protocol		
SAN.021	The switch should support Front to back and back to Front airflow		
SAN.022	The switch should have industry's most efficient power consumption i.e.0.14 watts/Gbps 110W with all 48 ports populated @16G		
SAN.023	The switch should have industry's lowest latency 700 ns through cut through routing technology		
SAN.024	The switch should have maximum 8000 plus buffers		
SAN.025	The switch should support in flight Compression and Encryption		
SAN.026	The Switch should have a DC Power option model		
SAN.027	The switch shall be optionally supplied with a GUI management software , capable of managing more than 36 fabrics and 2500 to 15000 ports		

2.30 Storage

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
STORE.001	Solution/ Type	IP Based/iSCSI/FC/NFS/CIFS		
STORE.002	Storage	▪ Storage Capacity should be minimum 1.25 PB (usable, after configuring in offered RAID configuration) and planned for the capacity required for all suggested applications ▪ RAID solution offered must protect against double disc failure. ▪ Disks should be preferably minimum of 3 TB capacity ▪ To store all types of data (Data, Voice, Images, Video, etc.) ▪ Storage system capable of scaling vertically and horizontally		
STORE.003	Hardware Platform	▪ Rack mounted form-factor ▪ Modular design to support controllers and disk drives expansion		
STORE.004	Controllers	▪ At least 2 Controllers in active/active mode ▪ Controllers / Storage nodes should be seamlessly upgradable, without any disruptions / downtime to production workflow, capacity enhancement and software / firmware upgrades.		
STORE.005	RAID support	RAID 0, 1, 1+0, 5+0 and 6		
STORE.006	Cache	Minimum 128 GB of useable cache across all controllers. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.		
STORE.007	Redundancy and High Availability	Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
STORE.008	Management software	▪ All necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. ▪ Licenses for storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, up to max capacity of the existing controller/units. ▪ A single command console for entire storage system. ▪ Should also include storage performance monitoring and management software ▪ Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures Should be able to take "snapshots" of the stored data to another logical drive for backup purposes		
STORE.009	Data Protection	Storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours		

2.31 Smart Rack for OCC

Smart Rack				
Sr. No.	**Item**	**Minimum Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
SROCC-01	Scale and Density of Integrated Data Center	7 to 8 KW IT load for 2 Rack Integrated DC with minimum 60U available for IT equipment's.		
SROCC-02	Inbuilt redundancy compliant to Tier 2/3 guidelines	Compliant to Tier 2/3 guidelines for Data Center, N + N redundancy for cooling system , Fire Detection & Suppression, PDU, Electrical DB, Water leakage detection and Monitoring system with Auto door opening, providing high availability of each equipment for set of 2 Rack Integrated DC.		
SROCC-03	Main Electrical Panel & Cabling	DB panel mounted inside cabinet with all internal cabling integrated into the same. Adequate precaution and compliances to be taken care for sizing/ratings of cables and switchgear inside Rack.		
SROCC-04	Uninterrupted Power Supply(UPS)	Rack mount on line double conversion UPS of 10 KVA up to 94% efficiency at full load and 0.8 output power factor. UPS to be provided with External battery bank with SMF batteries for 30 min. backup on 100% IT load with required rack mount accessories. UPS should follow all standards including UL/CE, ISO 9001 and ISO 14001		
SROCC-05	Cooling System	The cooling system shall be zero U rack based type with horizontal uniform cold air distribution with N+N redundancy.		
		It shall be highly efficient, closed loop circuit, “front to back” cooling solution up to 7kW per cooling unit with ambient temperature range +10° C to +50° C .		
		The cold air distribution shall be lateral, uniform from 1U to 42U in front of the 19” equipment for efficient cooling.		
		There shall be no loss of vertical “U” space inside the 19” Rack while mounting the equipment		
		Indoor operating temperature range: +18°C to +29°C		

Smart Rack				
Sr. No.	**Item**	**Minimum Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
		Indoor Unit Noise Level:49 dBA		
		Voltage Requirements: 1ph, 230V, 50Hz		
		Rack U space utilization: Zero U		
		Cooling Capacity Range: 5-8 kW		
		Outdoor Operating temperature range : +5°C to +50°C		
		Refrigerant: R407C		
		Outdoor Unit Noise Level :<60dBA		
		Voltage Requirements: 1ph, 230V, 50Hz		
		Compressor: Energy Efficient Fixed Speed Scroll Compressor Mounted on Anti Vibration Bush.		
		Condenser tubing: Air cooled condenser with internally grooved copper tubing for better Heat transfer efficiency and anti-corrosive coating on aluminum fins.		
		Copper piping with insulation tube of elastomeric, nitrile foam between each sets of outdoor & indoor unit as per specification. Piping to be properly supported by MS clamp. All transmission wiring between indoor to outdoor unit is kept in PVC conduit.		
		Fans: Low noise axial fans with high air flow, high static head with minimum losses		
SROCC-06	Access Control	Biometric reader (with relevant software along with licenses if needed). Integrated DC Rack doors should have electromagnetic lock to permit only authorized persons to open the doors through finger print reader. Design to be as per TIA 942 guidelines		
SROCC-07	Integrated Fire Security & Suppression System	Fire detection and suppression system with Novec 1230 clean agent based, modular type fire suppression system to cover entire racks. Design should be as per NFPA standards guidelines.		
SROCC-08	Water leak detection	Integrated Rack Level Water leak Detection System for each Rack.		

Smart Rack				
Sr. No.	**Item**	**Minimum Requirement Description**	**Compliance (Yes / No)**	**Deviations / Remarks**
SROCC-09	‘U’ Usable Space	Minimum ‘U’ space to be available to mount IT equipment’s should be 60U for set of 2 Rack Integrated DC		
SROCC-10	Remote Monitoring	Rack mounted Remote monitoring system continuously collects critical information from network connected devices, temperature, humidity, door sensors and other dry contact monitoring. Based on pre-set parameters, automated alerts and messages are sent to the intended recipients. Remote monitoring system with SNMP, email notification, event alerts. Monitoring of Temperature, Humidity, Door Switch sensor, water leak sensor.		
SROCC-11	Racks & enclosures with PDU	Sturdy frame section construction, All profile edges are radiuses. Removable top & Bottom cover with Cable entry provision. Frames should be bayable, scalable and modular, High density with 42U as standard, complete with shelf, cable manager & blanking panels with PDU. Each Rack frame should be 42 U 19'' mounting type with minimum 2000 mm (Height) x 600 or 800 mm (Width) x 1200 mm (Depth). Rack design should be sturdy frame section; corners stiffened with welded MS die cast. Rack to be provided with all basic accessories like, blanking panels, baying kit, sliding keyboard tray, vertical cable manager as well as horizontal cable manager, earthing copper strip with insulators, PDU 32 amp vertical mounting with IEC type socket with 12 nos of IEC C13 Sockets & 4 nos IEC C19 Socket with 2.5 mtr power chord with 32A MCB. Each rack shall have minimum two such PDU's.		

2.32 Smart Rack for CCC

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SRCCC-01	Scale and Density of Integrated Data Center	30-35 KW IT load for 6 Racks Integrated DC with minimum 210U available for IT equipments.		
SRCCC-02	Inbuilt redundancy compliant to Tier 2/3 guidelines	Compliant to Tier 2/3 guidelines for Data Center, N + N redundancy for cooling system , Fire Detection & Suppression, PDU, Electrical DB, Water leakage detection and Monitoring system with Auto door opening, providing high availability of each equipment for set of 2 Rack Integrated DC.		
SRCCC-03	Main Electrical Panel & Cabling	DB panel mounted inside cabinet with all internal cabling integrated into the same. Adequate precaution and compliances to be taken care for sizing/ratings of cables and switchgear inside Rack.		
SRCCC-04	Uninterrupted Power Supply(UPS)	External On-line double conversion UPS of 40 KVA up to 94% efficiency at full load and 0.8 output power factor. UPS to be provided with External battery bank with SMF batteries for 10-15 min. backup on 100% IT load with required accessories. UPS should follow all standards including UL/CE, ISO 9001 and ISO 14001		
SRCCC-05	Cooling System	The cooling system shall be zero U rack based type with horizontal uniform cold air distribution with N+N redundancy.		
		It shall be highly efficient, closed loop circuit, “front to back” cooling solution up to 7kW per cooling unit with ambient temperature range +10° C to +50° C .		
		The cold air distribution shall be lateral, uniform from 1U to 42U in front of the 19” equipment for efficient cooling.		
		There shall be no loss of vertical “U” space inside the 19” Rack while mounting the equipment		
		Indoor operating temperature range: +18°C to +29°C		
		Indoor Unit Noise Level:49 dBA		
		Voltage Requirements: 1ph, 230V, 50Hz		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		Rack U space utilization: Zero U		
		Cooling Capacity Range : 5-8 kW		
		Outdoor Operating temperature range : +5°C to +50°C		
		Refrigerant: R407C		
		Outdoor Unit Noise Level :<60dBA		
		Voltage Requirements: 1ph, 230V, 50Hz		
		Compressor: Energy Efficient Fixed Speed Scroll Compressor Mounted on Anti Vibration Bush.		
		Condenser tubing: Air cooled condenser with internally grooved copper tubing for better Heat transfer efficiency and anti-corrosive coating on aluminum fins.		
		Copper piping with insulation tube of elastomeric, nitrile foam between each sets of outdoor & indoor unit as per specification. Piping to be properly supported by MS clamp. All transmission wiring between indoor to outdoor unit is kept in PVC conduit.		
		Fans :Low noise axial fans with high air flow, high static head with minimum losses		
SRCCC-06	Access Control	Biometric reader (with relevant software along with licenses if needed). Integrated DC Rack doors should have electromagnetic lock to permit only authorized persons to open the doors through finger print reader. Design to be as per TIA 942 guidelines		
SRCCC-07	Integrated Fire Security & Suppression System	Fire detection and suppression system with Novec 1230 clean agent based, modular type fire suppression system to cover entire racks. Design should be as per NFPA standards guidelines.		
SRCCC-08	Water leak detection	Integrated Rack Level Water leak Detection System for each Rack.		
SRCCC-09	'U' Usable Space	Minimum 'U' space to be available to mount IT equipment's should be 60U for set of 2 Rack Integrated DC		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SRCCC-10	Remote Monitoring	Rack mounted Remote monitoring system continuously collects critical information from network connected devices, temperature, humidity, door sensors and other dry contact monitoring. Based on pre-set parameters, automated alerts and messages are sent to the intended recipients. Remote monitoring system with SNMP, email notification, event alerts. Monitoring of Temperature, Humidity, Door Switch sensor, water leak sensor.		
SRCCC-11	Racks & enclosures with PDU	Sturdy frame section construction, All profile edges are radiuses. Removable top & Bottom cover with Cable entry provision. Frames should be bayable, scalable and modular, High density with 42U as standard, complete with shelf, cable manager & blanking panels with PDU. Each Rack frame should be 42 U 19'' mounting type with minimum 2000 mm (Height) x 600 or 800 mm (Width) x 1200 mm (Depth). Rack design should be sturdy frame section; corners stiffened with welded MS die cast. Rack to be provided with all basic accessories like, blanking panels, baying kit, sliding keyboard tray, vertical cable manager as well as horizontal cable manager, earthing copper strip with insulators, PDU 32 amp vertical mounting with IEC type socket with 12 nos of IEC C13 Sockets & 4 nos IEC C19 Socket with 2.5 mtr power chord with 32A MCB. Each rack shall have minimum two such PDU's.		

Annexure 3: CCTV based City Surveillance System

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

3.1PTZ Specifications

Sr. No.	Item	Minimum Requirement Description	Compliance	Deviations / Remarks
			(Yes / No)	
PTZ001	General Requirements	Camera should be manufacturer's official product line designed for 24x365 use. Camera and camera firmware should be designed and developed by same OEM.		
PTZ002	General Requirements	Camera should be based upon standard components and proven technology using open and published protocols		
PTZ003	Image Sensor with WDR	1/3.2” with True WDR, Progressive CMOS Sensor or better		
PTZ004	Resolution	Camera should be HD 1920 (w) x1080 (h)		
PTZ005	lens specs	Compatible to image sensor, Focal length 4.3–129 m, Auto Iris, Full HD (1080P), IR Corrected – Day / Night mode-Colour		
PTZ006	Minimum illumination	Colour: 0.3 lux, B/W: 0.05 lux or better		
PTZ007	Pre-set Positions	100 or better, Pre-set tour		
PTZ008	Pan	360° endless, 350°/s		
PTZ009	Tilt Range	Manual/programmable; speed: 350°/sec; angle :0-180° or proportional speed needs to be provided		
PTZ010	Zoom	30x optical zoom with 12x digital zoom		
PTZ011				
PTZ012	True Day and Night	Automatic with IR cut filter		
PTZ013	IRIS	Auto IRIS		
PTZ014	Video Compression and streams	Triple Stream of H.264 Main profile & 1 Stream of Motion JPEG		

Sr. No.	Item	Minimum Requirement Description	Compliance	Deviations / Remarks
			(Yes / No)	
PTZ015	Resolutions and frame rates (H.264)	Minimum 1920 x 1080 @ 25 fps (1080p) or better		
PTZ016	Power Supply	Power over Ethernet IEEE 802.3af		
PTZ017	Remote, Auto Focus support	Yes		
PTZ018	Local storage (S.D or Micro SD)	microSDXC memory card of 128GB (Class 10): In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.		
PTZ019	Supported Protocol	IPv4 & v6, HTTP, HTTPS**, SSL/TLS**, QoS Layer 3 DiffServ, FTP, CIFS/SMB,SMTP, UPnP™,SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP		
PTZ020	Security	IEEE 802.1x,Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
PTZ021	ONVIF	Profile S&G		
PTZ022	Operating Temp	0 to 55°C or better		
PTZ023	Backlight Compensation	Automatic		
PTZ024	Wide Dynamic Range	Minimum 100db		
PTZ025	Digital PTZ	Yes		
PTZ026	Intelligent video	Video motion detection, active tampering alarm		
PTZ027	Bandwidth Optimization	low bandwidth utilization without compromising image quality		
PTZ028	Housing	IP 66/65 Rated for outdoor use with internal /external IR illuminators which can cover up to 50 mts .Compliance to Vandal and impact resistant housing – IP66 / NEMA 4X, IK10		
PTZ029	Certifications	UL, CE,FFC and EN ,		

Sr. No.	Item	Minimum Requirement Description	Compliance	Deviations / Remarks
			(Yes / No)	
PTZ030	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, , Gain Control, , Electronic Image Stabilization,		
PTZ031	Text Superimposing:	Camera shall support superimposing the title and date & time on the video		
PTZ032	Intelligent video	Video motion detection, active tampering alarm		

3.2 Box Camera Specifications

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
FIXBOX 1	General Requirements	Camera should be based upon standard components and proven technology using open and published protocols		
FIXBOX 2	Image Sensor with WDR	1/2.9 “ ” with True WDR, Progressive CMOS Sensor or better		
FIXBOX 3	Vari-focal Lens	2.8 -8mm / 5-50mm lens		
FIXBOX 4	True Day and Night	Automatic with IR cut filter		
FIXBOX 5	IRIS	Auto P-IRIS		
FIXBOX 6	Video Compression and streams	Triple Stream of H.264 Main profile & 1 Stream of Motion JPEG		
FIXBOX 7	Resolutions and frame rates (H.264)	Minimum 3072 x 1728 @ 25 fps (5 Mp) or better		
FIXBOX 8	Power Supply	Power over Ethernet IEEE 802.3af		
FIXBOX 9	Remote, Focus support	Required		
FIXBOX 10	Local storage (S.D or Micro SD)	microSDXC memory card of 128GB (Class 10): In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording on request from VMS such that no manual intervention is required to transfer the SD card based recordings to server.		

Sr. No.	Item	Minimum Requirement Description	Compliance	Deviations / Remarks
			(Yes / No)	
FIXBOX 11	Supported Protocol	IPv4 & v6, HTTP, HTTPS**, SSL/TLS**, QoS Layer 3 DiffServ, FTP, CIFS/SMB,SMTP, UPnP™,SNMPv1/v2c/v3(MIB-II), DNS, DynDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP		
FIXBOX 12	Security	IEEE 802.1x,Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
FIXBOX 13	ONVIF	Profile S&G		
FIXBOX 14	Operating Temp	0 to 55°C or better		
FIXBOX 15	Wide Dynamic Range	Minimum 100db		
FIXBOX 16	Digital PTZ	Yes		
FIXBOX 17	Intelligent video	Video motion detection, active tampering alarm		
FIXBOX 18	Bandwidth Optimization	low bandwidth utilization without compromising image quality		
	Housing	Separate (not Integrated with camera) IP 66/65 Rated for outdoor use with internal /external IR illuminators which can cover up to 50 mts .Compliance to Vandal and impact resistant housing – IP66 / NEMA 4X, IK10		
FIXBOX 19	Certifications	UL, CE,FFC and EN ,		
FIXBOX 20	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight		

Sr. No.	Item	Minimum Requirement Description	Compliance	Deviations / Remarks
			(Yes / No)	
		compensation, Gain Control, , Electronic Image Stabilization, Auto Tracking		
FIXBOX 21	Text Superimposing:	Camera shall support superimposing the title and date & time on the video		
FIXBOX 22	Intelligent video	Video motion detection, active tampering alarm		
FIXBOX 23	Bandwidth Optimization	low bandwidth utilization without compromising image quality		

3.3Video Management System

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
VMS.001	General Requirements	VMS shall work on ONVIF Open Platform catering to all the security needs of city		
VMS.002	General Requirements	VMS shall be open to any ONVIF IP cameras integration so that it would be able to cater future requirements of the project		
VMS 003	General Requirements	VMS shall support interoperability of IP cameras from multiple vendors		
VMS 004	General Requirements	Bidders shall clearly mention in their proposal the brands and models integrated into VMS		
VMS 005	General Requirements	VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.		
VMS 006	General Requirements	VMS system shall cluster the processing & memory load across several machines. The failure of any one server in the solution shall not cause a failure in the entire system.		
VMS 007	General Requirements	System shall allow the frame rate, bit rate and resolution of each camera to be configured independently for recording.		
VMS 008	General Requirements	System shall support H.264and MJPEG compression formats for all IP cameras connected to the system.		
VMS.009	General Requirements	Video Management System shall support high availability of recording servers. A failover option shall provide standby support for recording servers with automatic synchronization to ensure maximum uptime and minimum risk of lost data.		
VMS.010	General Requirements	Video Management System software shall have multicast and multi-streaming support. It shall definitely have the ability to take a snapshot from any online live camera and export to a standard graphic file format.		
VMS.011	General	Video Management System shall support archiving for optimizing recorded data		

	Requirements	storage through unique data storage solutions by combining performance and scalability with cost efficient long-term video storage.		
VMS.012	General Requirements	VMS shall be ONVIF compatible		
VMS.013	Forensic Requirment	VMS shall Attribute base search on at least 30% of cameras to search the person on the basis of attribute like gender, type and colour of clothes and image of person from the CCTV feeds and should able to run on multiple cameras to track the person		

3.4 Dome Camera Specifications

Sr.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/ Remarks
DM01	Video Compression	H.264		
DM02	Video Resolution	3072x1728		
DM03	Frame rate	2 MP: 25 FPS, 3 MP @ 20FPS & 5 MP @ 1212 fps		
DM04	Image Sensor	1/3" Progressive Scan CMOS		
DM05	Lens	Autofocus, P- IRIS 3-9 mm , F1., remote zoom and focus, IR corrected		
DM06		Colour: 0.2 lux, B/W: 0.05 lux (at 30 IRE)		
DM07	Day/Night Mode	Colour, Mono, Auto		
DM08	S/N Ratio			
DM09	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, Gain Control, Auto back focus		
DM010	Wide Dynamic Range	True WDR up to 90 db		
DM011	Audio	Full duplex, line in and line out, G.711, G.726		
DM012	Local storage	microSDXC memory card of 32GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording on request from VMS such that no manual intervention is required to transfer the SD card based recordings to server.		
DM013	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, Profile S &G		
DM014	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		

Sr.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/ Remarks
DM015	Intelligent Video	Motion Detection & Tampering alert		
DM016	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
DM017		0 to 50°C		
DM018		IP66 and IK10 rated		
DM019		UL, CE ,FCC		
DM020		802.3af PoE		
DM021	Sustainability	PVC Free		
DM022	Memory	512 MB RAM, 128 MB Flash		
DM023	Analytics Included	Motion Detection, Active Tampering Alarm, Audio Detection		
DM024	Analytics	Should Support Installation of Thirdparty applications		

3.5 Pole for cameras

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
POLE.001	General Requirement	NHAI norms and guideline must be follow		
POLE.002	General Requirement	Hot dip galvanized pole with minimum 5mm to 10 mm thickness , as per indicated in the indicative drawing		
POLE.003	Foundation	Pole would be fixed on an adequate and strong pre-cast foundation to withstand city weather conditions and wind speed of 150 km/hr		
POLE.004	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		
POLE.005	Sign Board with number plate	Sign board depicting the area under surveillance and with serial number of pole		
POLE.006	Height	Height of the pole shall be as per requirement of the location varying from 6 m to 12/15 m.		
POLE.007	Electrical Connection	Electrical power requirement for the systems/devices installed on the pole should be available with metering and protection equipment		
POLE.008	Lightning Protection	Lighting arrestors with proper grounding		
POLE.009	Earthing	Pole should have proper earthing system		
POLE.010	Network Communication	All communication passive & active devices should be housed in enclosure of adequate standards and protection		

3.6Pole for cameras (Junction box)

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
POLJB.001	General Requirement	All the junction boxes shall be out door type with **IP65** protection from rain, water. Provision for theft prevention.		
POLJB.002	General Requirement	Separate junction box for DC redundant power supple and battery and 230-volt input connection Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet.		
	General Requirement	Opening lever/handles shall be made of metal.		
POLJB.004	General Requirement	Cabinet dimension as per indicated in the Indicative drawing		
POLJB.005	General Requirement	Junction box shall electromagnetic lock which can be open remotely form control and command center as well as vandal proof locking system		
POLJB.006	General Requirement	Advertisement board as per indicated in Indicative drawing		
POLJB.007	General Requirement	Rain canopy on Top with all around projection of the enclosure such that that rain water, water logging shall not penetrate in the junction box and hamper working of the system, cable entry with glands.		
POLJB.008	General Requirement	Small Junction box for mounting Electrical Meter, Fuse and MCB with separate lock for utility power connection		
POLJB.009	General Requirement	Protection from ants, bugs and other small insects entering the enclosure		
POLJB.010	Standard and Support	Regulatory Standard Compliance: IP55/65 and The system should not be an end of life / end of service product.		

Annexure 4: Biometric Attendance System

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

4.1 Fixed Finger Scanner Specifications

Sr.No.	Parameters	Specifications	Compliance (YES/NO)	Deviations /Remarks
FFS1	Screen	Minimum 4” QVGA Colour Touch Screen with positioning guidance		
FFS 2	Audio Support	Equipped with speakers for audio support and customizable voice prompts		
FFS 3	Camera	Capable of capturing user’s face using invisible near-infrared light pattern even in in poor lighting conditions		
FFS 4	Imaging Technology	Device should use real-time 3D imaging technology		
FFS 5	Tolerance	Inbuilt tolerance to facial angles and motion that can interpret 3D facial biometric matching		
FFS 6	Security	Security provisions to detect device tampering and attempts to spoof the system and create a log & trigger alert		
FFS 7	Operating Conditions	Operating Temperature 5°C to 50°C		
FFS 8	Communication	for LAN, WAN through RS485 port and for PC connection through USB & RS232 port		
FFS 9	Event log	Capable of Logging events for audit trails		
FFS 10	False Accept Rate	0.00001% in 1:1 mode		
FFS 11	Interface	Capable of interfacing directly with other applications and devices using Wiegand, RS232, RS422 or RS485 interfaces		
FFS 12	Audio Port	In built Speaker with 1W or above Speaker Supporting WAV Files		
FFS 13	Operating System	Android OS 4.2 or above /Linux OS latest version		
FFS 14	Data Ports	USB 2.0 & RS-232, RJ45/Ethernet)/Wi-Fi		
FFS 15	Protocol	TCP/IP / HTTP /HTTPS		
FFS 16	Immunity	IEC 61000-4-2, Level 3; IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-9, all Level 4		

Sr.No.	Parameters	Specifications	Compliance (YES/NO)	Deviations /Remarks
FFS 17	IP 65 Compliant & Compact	Device should be rugged enough for field usage and weight should not be more than 350 gms. Easy to carry in field. Water and dust proof. IP 65 Certification to be provided.		
FFS 18	Finger Print Scanner	High Performance Optical Sensor (500dpi), STQC Certified		
FFS 19	Best Detection Finger client	BFD client application conforming to Aadhaar Best Finger Detection (BFD) API 1.6. BFD application should have capability of displaying NFIQ score of each finger.		
FFS 20	Platen	Rugged, minimum IP 54 rating preferable Prefer scratch resistant Features		
FFS 21	NFIQ Quality Software	Inbuilt NFIQ quality software either at device level or extractor level.		
		High Quality Image (NFIQ<=2) in dry, wet, dirt, oil dry and bright light conditions		
FFS 22	Audio/Visual	Indication either at device level or at application level for indicating various events like:		
FFS 23	Indication	(a) Indication for placing finger. (b)Start of capturing. (c) End of capturing.		
FFS 24	SDK support	To provide all SDKs for the devices like Finger Printer Biometric etc. Software API: Compliant with UIDAI Device Capture API specification V1.0 RC 3. Supplier shall provide all necessary technical support for integration of the device drivers with the various applications.		
FFS 25	Finger Capture Device performance:	The sensor shall have failure to enrolment rate (FTE) of 0.01% The sensor shall have no or very low failure to acquire rate (FTA) of 0.001%.		
FFS 26	Others	The sensor shall be able to generate good quality image and produce high scores on recommended test procedures /standards for more than 95% of the time, for different real world operating conditions		

4.2 Mobile Finger Scanner

Sr.No.	Parameters	Specifications	Compliance (YES/NO)	Deviations/Remarks
MFS 1	Micro Processor	Latest High Speed Processor. Capable to support Latest Android OS/ Latest Linux OS		
MFS 2	CPU Speed & RAM	1 GHz or more; Minimum RAM 1 GB or higher		
MFS 3	Flash Memory	Minimum 4GB Upgradable up to 32 GB		
MFS 4	LCD	3.5 Inch Touch Screen TFT LCD 320 X 3(RGB) X 240 pixels; with sunlight readability.		
MFS 5	Keyboard	30 Keys Alphanumeric bigger Keyboard -(easy to operate Keyboard)		
MFS 6	Battery	Lithium-Polymer/Lithium –Ion with minimum 4500 mAh above suitable for minimum 8 hours operation. Life: 300 cycles.		
MFS 7	Charger	AC 180V to 240V charger for 3 to 4 hours charging.		
MFS 8	SIM card provision	1 No		
MFS 9	Cabinet	Aesthetically designed ABS or Poly Carbonate plastic Housing, with integrated, LCD display, Fingerprint sensor and Keyboard etc.		
MFS 10	GPS	Inbuilt GPS Module with minimum 30 channels, support AGPS and DGPS anti jamming, cold start time less than 40 Sec, low power consuming and provide location details within the range of 100 meters area.		
MFS 11	SD Card Provision	SD Card Holder to extend Memory up to 32 GB		
MFS 12	Communication	GPRS with 4G (mandatory)		
MFS 13	Audio Port	In built Speaker with 1W or above Speaker Supporting WAV Files		
MFS 14	Operating System	Android OS 4.2 or above /Linux OS latest version		
MFS 15	Data Ports	USB 2.0 & RS-232 (optional)		
MFS 16	Protocol	TCP/IP / HTTP /HTTPS		
MFS 17	Immunity	IEC 61000-4-2, Level 3; IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC 61000-4-9, all Level 4		

Sr.No.	Parameters	Specifications	Compliance (YES/NO)	Deviations/Remarks
MFS 18	IP 65 Compliant & Compact	Device should be rugged enough for field usage and weight should not be more than 350 gms. Easy to carry in field. Water and dust proof. IP 65 Certification to be provided.		
MFS 19	Finger Print Scanner	High Performance Optical Sensor (500dpi), STQC Certified		
MFS 20	Best Detection Finger client	BFD client application conforming to Aadhaar Best Finger Detection (BFD) API 1.6. BFD application should have capability of displaying NFIQ score of each finger.		
MFS 21	Platen	Rugged, minimum IP 54 rating preferable Prefer scratch resistant Features		
MFS 22	NFIQ Quality Software	Inbuilt NFIQ quality software either at device level or extractor level. High Quality Image (NFIQ<=2) in dry, wet, dirt, oil dry and bright light conditions		
MFS 23	Audio/Visual Indication	Indication either at device level or at application level for indicating various events like: (a) Indication for placing finger. (b)Start of capturing. (c) End of capturing.		
MFS 24	SDK support	To provide all SDKs for the devices like Finger Printer Biometric etc. Software API: Compliant with UIDAI Device Capture API specification V1.0 RC 3. Supplier shall provide all necessary technical support for integration of the device drivers with the various applications.		
MFS 25	Finger Capture Device performance:	The sensor shall have failure to enrolment rate (FTE) of 0.01% The sensor shall have no or very low failure to acquire rate (FTA) of 0.001%.		
MFS 26	Others	The sensor shall be able to generate good quality image and produce high scores on recommended test procedures /standards for more than 95% of the time, for different field operating real world conditions		

4.3Smart Rack for AMC

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SRAMC-01	Scale and Density of Integrated Data Center	4-5 KW IT load for Single Rack Integrated DC with minimum 28U available for IT equipments.		
SRAMC-02	Inbuilt redundancy compliant to Tier 2/3 guidelines	Compliant to Tier 2/3 guidelines for Data Center, N + N redundancy for cooling system , Fire Detection & Suppression, PDU, Electrical DB, Water leakage detection and Monitoring system with Auto door opening, providing high availability of each equipment for set of 2 Rack Integrated DC.		
SRAMC-03	Main Electrical Panel & Cabling	DB panel mounted inside cabinet with all internal cabling integrated into the same. Adequate precaution and compliances to be taken care for sizing/ratings of cables and switchgear inside Rack.		
SRAMC-04	Uninterrupted Power Supply(UPS)	Rack mount on line double conversion UPS of 6 KVA up to 94% efficiency at full load and 0.8 output power factor. UPS to be provided with Internal battery bank with SMF batteries for 10-15 min. backup on 100% IT load with required rack mount accessories. UPS should follow all standards including UL/CE, ISO 9001 and ISO 14001		
SRAMC-05	Cooling System	ü The cooling system shall be zero U rack based type with horizontal uniform cold air distribution with N+N redundancy.		
		ü It shall be highly efficient, closed loop circuit, “front to back” cooling solution up to 7kW per cooling unit with ambient temperature range +10° C to +50° C .		
		ü The cold air distribution shall be lateral, uniform from 1U to 42U in front of the 19” equipment for efficient cooling.		
		ü There shall be no loss of vertical “U” space inside the 19” Rack while mounting the equipment		
		ü Indoor operating temperature range: +18°C to +29°C		
		ü Indoor Unit Noise Level:49 dBA		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		ü Voltage Requirements: 1ph, 230V, 50Hz		
		ü Rack U space utilization: Zero U		
		ü Cooling Capacity Range : 5-8 kW		
		ü Outdoor Operating temperature range : +5°C to +50°C		
		ü Refrigerant : R407C		
		ü Outdoor Unit Noise Level : <60dBA		
		ü Voltage Requirements : 1ph, 230V, 50Hz		
		ü Compressor: Energy Efficient Fixed Speed Scroll Compressor Mounted on Anti Vibration Bush.		
		ü Condenser tubing: Air cooled condenser with internally grooved copper tubing for better Heat transfer efficiency and anti-corrosive coating on aluminum fins.		
		Copper piping with insulation tube of elastomeric, nitrile foam between each sets of outdoor & indoor unit as per specification. Piping to be properly supported by MS clamp. All transmission wiring between indoor to outdoor unit is kept in PVC conduit.		
		ü Fans :Low noise axial fans with high air flow, high static head with minimum losses		
SRAMC-06	Access Control	Biometric reader (with relevant software along with licenses if needed). Integrated DC Rack doors should have electromagnetic lock to permit only authorized persons to open the doors through finger print reader. Design to be as per TIA 942 guidelines		
SRAMC-07	Integrated Fire Security & Suppression System	Fire detection and suppression system with Novec 1230 clean agent based, modular type fire suppression system to cover entire racks. Design should be as per NFPA standards guidelines.		
SRAMC-08	Water leak detection	Integrated Rack Level Water leak Detection System for each Rack.		
SRAMC-09	‘U’ Usable Space	Minimum ‘U’ space to be available to mount IT equipment’s should be 60U for set of 2 Rack Integrated DC		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
SRAMC-10	Remote Monitoring	Rack mounted Remote monitoring system continuously collects critical information from network connected devices, temperature, humidity, door sensors and other dry contact monitoring. Based on pre-set parameters, automated alerts and messages are sent to the intended recipients. Remote monitoring system with SNMP, email notification, event alerts. Monitoring of Temperature, Humidity, Door Switch sensor, water leak sensor.		
SRAMC-11	Racks & enclosures with PDU	Sturdy frame section construction, All profile edges are radiuses. Removable top & Bottom cover with Cable entry provision. Frames should be bayable, scalable and modular, High density with 42U as standard, complete with shelf, cable manager & blanking panels with PDU. Each Rack frame should be 42 U 19'' mounting type with minimum 2000 mm (Height) x 600 or 800 mm (Width) x 1200 mm (Depth). Rack design should be sturdy frame section; corners stiffened with welded MS die cast. Rack to be provided with all basic accessories like, blanking panels, baying kit, sliding keyboard tray, vertical cable manager as well as horizontal cable manager, earthing copper strip with insulators, PDU 32 amp vertical mounting with IEC type socket with 12 nos of IEC C13 Sockets & 4 nos IEC C19 Socket with 2.5 mtr power chord with 32A MCB. Each rack shall have minimum two such PDU's.		

Annexure 5: Smart Transport system & Smart Bus Stops

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

5.1 Bus Stop Specifications

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
Smart Bus Shelter-Type A (Size: 6X2mts.)				
BUS.001	General Requirements: **Location**	The location of Type A bus shelters will be shared by AMC/SPV.		
BUS.002	General Requirements: **Functioning and sizing**	Bus Shelter – BS shall serve as an all weather shade for the bus commuters and the Shelter area shall not exceed 12sqm. The structure shall be designed to withstand wind load, structural load according to Indian standard regulations (IRC; MoRTH). The display systems can have fixed or scrolling faces with back light		
BUS.003	General Requirements: **Materials**	Bus shelter shall be made of MS frame work, powder coated metal roofing, metal seating, toughened glass/ acrylic and electronic circuit to control its lighting. All the steel parts shall be HDG –Hot dip galvanized and aluminum parts shall be anodized or powder coated to give longer life and better quality. The material used shall be unaffected by outdoor exposure The material shall be Non flammable. The Foundation slab shall be made in min M25 concrete. The cast iron nuts, bolts shall be rust proof , deep galvanized powder coated etc.		
BUS.004	General Requirements: **Maintenance**	The furniture shall be maintained by washing and periodic servicing. The display shall be covered using toughened glass/ acrylic, with protective frames on its edges which shall be also cleaned periodically.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		The poles and metal parts shall be coated for protection in case found damaged.		
BUS.005	General Requirements: **Vandalism Proof**	The Parts used shall not be fragile and safely secured to its foundation with anchor fasteners which makes the furniture more stable and joint fasteners not visible from outside. None of the joints shall be visible from outside the furniture and it is completely sealed. Opening shall be by specialized key.		
BUS.006	General Requirements: **Security and safety**	There shall be no falling parts, no sharp edges involved in the furniture all the parts shall be well fastened. The foundation used shall be designed in order to take loads from wind and persons leaning over the panel.		
BUS.007	General Requirements: **Durability**	The parts used shall be of mild steel, stainless steel, aluminum, toughened glass or acrylic for better durability. The mild steel, stainless steel, and aluminum shall be treated to be resistant in all weathers.		
BUS.008	General Requirements: **Co-ordinated design**	All BS shall be of uniform shape, size, facilities on the same width of footpath.		
BUS.009	General Requirements: **Eco-Friendly**	As far as possible Locally available and/or recyclable materials shall be used for making of the bus shelter.		
BUS.010	General Requirements: **Universal design**	The Bus shelter design should cater to differently abled users. Design and manufacture should comply with ISO requirements.		
BUS.011	Additional Infrastructure: **Road Marking**	Bus stop marking- Marking dimensions 3.5m(W)x18m(L)Providing and Laying of PLASTITRAK,Roll-on Surfacing Material -A Solvent Free, High Build, Two pack, Seamless, Tough, skid resistant 1.0-1.5 mm thick red (or as required) based on Gloss and color retaining Acrylic Cross Linking		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		Resin System for Bus stop and similar applications including surface cleaning and cost of all material etc. complete. Execution of work as directed by Engineer In-charge.		
BUS.012	Additional Infrastructure: **Footpath***	Paver Block- Providing and laying 60mm thick factory made cement concrete paver block (shot blasted finish) of M -30 grade in Footpath made by block making machine with strong vibratory compaction, of approved size, design and shape, laid in required color and pattern over and including 50mm thick compacted bed of coarse sand(pana) with base of 150 mm compacted GSB, filling the joints with fine sand etc. all complete as per the direction of Engineer-in charge, as per clause 410 of MoRTH Specification (Vth Revision) including cost, conveyance, of all materials, TandP, labor etc.,		
BUS.013	Additional Infrastructure: **Kerb***	Providing 100mm thick readymade c.c. kerb of strength M-20 (size 300mm x 380mm)purchased from AMC's approved paver block manufacturer and setting in line, level and in truly vertical position, including filling joints in C.M. 1-1 (1 part of cement - 1 part of stone dust)smooth pointing in C.M. 1-1 (1 part of cement - 1 part of coarse sand) including watering etc. complete and as directed by engineer in charge.		
BUS.014	Additional Infrastructure: **Kerb paint***	Painting two coats with Synthetic Enamel paint over a coat of enamel primer on concrete surface including cost, conveyance, taxes, of all materials, TandP,labour etc.as per technical Specification in clause 803 of MoRTH (Vth Revision) and as per direction of Engineer-In-Charge.		
BUS.015	Additional Infrastructure: **Tactile flooring***	Supply and laying of Cement Concrete Wet Cast Chequered Tiles 300 x 300 x 30mm, Colour as approved by AMC and to be UV light resistant. Chequered Tiles must confirm to IS 13801-1993. Installation includes 150mm GSB base with 50 mm 1-2-4 PCC base and 1-5 mortar mix for fixing of tiles with level to match with footpath concrete paver blocks and		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		as directed by Engineer in charge. Item also includes all materials, labour, equipments, tools, watering, cleaning etc. complete. Scope of work also includes strong vibratory compaction.		
BUS.016	Facilities: **Bench with planters**	Provision at Bus stops, as directed by Engineer In-charge. Supply and install Bench/ Public seating for min. 5 persons along with a stainless steel planter(along with the shrub as selected by AMC/SPV) on either side of the bench; SS SF 304, for a rust free life. The Foundation slab shall be made in min M25 concrete. The cast iron nuts, bolts, shall be rust proof deep galvanized powder coated etc The stainless steel shall be treated to be resistant in all weathers.		
BUS.017	Facilities: **Dual system Litter Bins**	Provision at Bus stops, as directed by Engineer In-charge. Supply and install Dual Bin system make SS SF 304, for a rust free life capacity of 50ltrs each. The Foundation slab shall be made in min M25 concrete. The cast iron nuts, bolts, shall be rust proof deep galvanized powder coated etc The stainless steel shall be treated to be resistant in all weathers.		
BUS.018	Facilities: **Vending Kiosk (manned)**	The size of Kiosk shall be 2mts. x 2mts and it should be incorporated within the bus shelter space of 12 sqm. The kiosk shall have display racks, storage space and a back lit display panel. The kiosk shall have natural ventilation and a sturdy roof to protect from sunlight and rain. The height of the kiosk between ground and canopy shall be at-least 2.25mts, and location should be such that it doesn't hinder the pedestrian movement/vision. Materials used shall be steel/aluminum with anti corrosion treatment. Installation as directed by Engineer In-charge.		
BUS.019	Smart Infrastructure: **PTZ Camera**	Refer to technical specification for PTZ Camera		
BUS.020	Smart Infrastructure: **PIS**			

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
BUS.021	Smart Infrastructure: **WiFi**			
BUS.022	Smart Infrastructure: **Solar panels**			
BUS.023	Smart Infrastructure: **Emergency call box**	Refer to technical specification for Emergency call box		
BUS.024	Smart Infrastructure: **LED Lighting**			

Note: *In case of absence of footpath and/or kerb, the bidder has to consider the mentioned components for bidding and execution purpose

5.2 Roof Top Solar Panel for smart Bus Stop

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
RTSOP.001	PV Modules – BIS Standards	PV modules used must qualify to the latest edition of IEC PV module qualification test or equivalent BIS standards Crystalline Silicon Solar Cell Modules IEC 61215/IS14286. In addition, the modules must conform to IEC 61730 Part-1 - requirements for construction & Part 2 – requirements for testing, for safety qualification or equivalent IS.		
RTSOP.002	Operating Conditions	PV modules must qualify to IEC 61701. Modules shall be made of light weight cells, resistant to abrasion, hail impact, rain, water and environmental pollution. PV modules shall be provided with anti-reflection coating		
RTSOP.003	Panel Capacity	Each panel should comprise of solar crystalline modules of minimum 300 Wp and above		
RTSOP.004	Protective Devices	Protective devices against surges at PV module shall be provided. Low voltage drop bypass diodes shall be provided.		
RTSOP.005	Module Certification	PV modules must be tested and approved by IEC authorized test centers.		
RTSOP.006	Module Frame	Module frame shall be made of corrosion resistant materials, preferably/ shall be anodized aluminum.		
RTSOP.007	Module Efficiency	Efficiency of PV modules at standard test conditions (STC) shall not be less than 15.5% and fill factor of the module shall not be less than 0.80.		
RTSOP.008	Output Power	Rated output power of any supplied module shall have tolerance within +/-3%.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
RTSOP.009	Variation in Voltage/ Current	Peak-power point voltage/current of any module/ string (series connected modules) shall not vary by more than 2 % from respective arithmetic means for all modules/ strings		
RTSOP.010	Junction Box	▪ Junction box shall have hinged, weather proof lid with captive screws and cable gland entry points or may be of sealed type and IP-65 rated. ▪ Each Junction Box shall have High quality Suitable capacity Metal Oxide Varistors (MOVs) / SPDs, suitable Reverse Blocking Diodes ▪ Array Junction Box shall have isolator that will be used to disconnect both positive and negative sides simultaneously on output side. ▪ Array Junction Box shall have the sensors to monitor parameters such as Analog signals: String currents, String Voltage & Digital signals: Isolator ON/OFF status		
RTSOP.011	Mounting Structure	Structures shall resist worst combination of specified loads / stresses under test and working conditions; these include dead load, live load, equipment load, water pressure, soil pressure, wind load, seismic load, stresses due to temperature changes, shrinkage and creep in materials, dynamic loads.		
RTSOP.012	Mounting Structure	Hot dip galvanized MS mounting structures shall be used for mounting modules/ panels/arrays. Each structure should have angle of inclination as per the site conditions to take maximum insulation.		
RTSOP.013	Mounting Structure	▪ Environmental condition shall be as per IS 456, IS 800. ▪ Individual members of frame shall be designed for worst combination of forces such as bending moment, axial force, shear force and torsion as applicable.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes/No)	Deviations / Remarks
		▪ Permissible stresses for different load combinations shall be as per latest IS456.		
RTSOP.014	Mounting Structure	Mounting structure steel shall be as per latest IS 2062: 1992 and galvanization of mounting structure shall be in compliance of latest IS 4759.		
RTSOP.015	Mounting Structure	Structural material shall be corrosion resistant and electrolytically compatible with materials used in module frame, its fasteners, nuts and bolts. Necessary protection towards rusting need to be provided by coating		
RTSOP.016	Cable Termination & Fuse	▪ All wires/cables must be terminated through cable lugs. Copper bus bars/ terminal blocks housed in the junction box with suitable termination threads conforming to IEC 62208 Hinged door with EPDM rubber gasket to prevent water entry. ▪ Fuses shall be provided on positive & negative terminal of incoming string. ▪ All fuses (Input Side) shall have DIN rail mountable fuse holders and shall be housed in thermoplastic IP 65 enclosures with transparent covers.		
RTSOP.017	RF Identification Tag	Modules deployed must use a RF identification tag with information regarding the details of manufacturing.		
RTSOP.018	PV Module Warranty	Should warrant the Solar Module(s) to be free from defects/failures specified below for a period not less than five years from the date of installation.		
RTSOP.019	Performance Warranty	Predicted electrical degradation of power generated not exceeding 20% of minimum rated power over 25 year period and not more than 10% after ten years period of full rated original output.		

5.3Led display system for PIS

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
DIDIS.001	Infrastructure requirement	Should comprise of Hardware based Clients, management platform, network infrastructure to deliver multimedia content through Digital full Colour LED Display Panel to Citizens.		
DIDIS.002	CMS Requirement	Should be enterprise-grade configurable and manage web clients designed to deliver multimedia services for public venues, including high- definition digital displays and panels.		
DIDIS.003	Platform Requirement	Should feature a web browser, which is a comprehensive web-centric		
		Application development platform with integrated Java Script API access to multimedia, peripheral, and system resources.		
		Support for plug-ins such as Adobe Flash Player, the browser should provide several proprietary widgets, which can be configured and controlled from JavaScript, Applications to be displayed in templates that also contain zones for Really Simple Syndication (RSS) feeds and advertising content. Built-in support for voice and video communication Devices should be configurable and managed remotely by web-based management portal with a menu- based GUI. Screens should operate basic content in case it gets disconnected from central manager.		
DIDIS.004	Physical form	Screens should be in a protective shell made of robust weatherproof material;		
		Screens would be placed outdoor so it should survive adverse weather condition.		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		Arrangements for safety and security of the Digital Outdoor LED Display Screens.		
DIDIS.005	Security requirements	System should have role based access control for secured and control user access. Should ensure that any data stored within or being transferred is encrypted as per industry standards with no data loss Screens to be equipped with sufficient tamper-proof mechanisms to ensure detection in case of physical tampering		
DIDIS.006	Screen	Resolution 1920 x 1080 & Aspect Ratio 16: 9 & Display Colours 16.7M & Brightness (cd/m^2)/(typ) minimum 2,500 Contrast Ratio (Native) 5000: 1 Response Time (ms, GTG) Viewing Angle Y̊ /V̊) 6 178°/178° Operational Hours Embedded player 24 X 7 Temperature, Brightness Sensor & Backlight type: LED/LCD Built in speaker 10 + 10 Protective Grade IP65 & UV Protection Shield Enabled Operating System Windows/ Linux		
DIDIS.007	Display Input	VGA (15 pin D-Sub) 1, HDMI 2, DVI & DP 1 & USB & RJ45 1 Wi-Fi Embedded: RS-232C 1 Refresh Frequency ≥1200Hz or 2800Hz, Refresh Rate: 2000 Hz & Frame Frequency: 50-60 Hz Input Voltage: AC 220V/50 Hz or AC 110V/60 Hz & Power Consumption: Average: 300 W/m^2; Max: 600 W/m^2 Defects Rate: ≤ 0.00001		

Sr. No.	Item	Minimum Requirement Description	Compliance (Yes / No)	Deviations / Remarks
		⍰ MTBF> 10000 hrs & Life Span ≥ 100000 hrs		
DIDIS.008	Power Requirement	⍰ Operating Voltage: 100 - 240VAC ⍰ Display Consumption (maximum): 940 ⍰ Digital Outdoor LED Display Screens Auto Cooling System ⍰ PIR Sensor (Motion detection): Optional ⍰ Luminance Sensor (Auto Brightness) ⍰ Temperature: 0 -50 °C ⍰ Humidity (non-condensing): 20 – 95 % ⍰ Earth leakage current < 3mA		
DIDIS.009	Certification Required	ULL, CE certification (ii) BIS certification for LED panels,		

Annexure 6: City Wi-Fi

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

6.1Wifi Specifications

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
City Wi-Fi				
FUNCTIONAL REQUIREMENTS				
General				
WIFI.001	**Functional Requirement**	City wide Wi-Fi Network shall comprise of the following components: • Access Points (APs) including the mounting infrastructure • Wireless Controllers • Wi-Fi Management System • Associated active and passive infrastructure		
WIFI.002	**Functional Requirement**	City-wide Wi-Fi shall have a secure, seamless and redundant network. It shall support industry standard based two (2) step authentication procedure.		
WIFI.003	**Functional Requirement**	City-wide Wi-Fi services shall be provided across all public spaces and other strategic locations in consultations with the Client.		
WIFI.004	**Functional Requirement**	The target bandwidth proposed per end-user is 2 Mbps throughout the City on a per session basis for the 30 minutes or 50 MB per session that will be given to the user at no cost.		
WIFI.005	**Functional Requirement**	The system shall be designed for scalability and allow future expansions in terms of subsequent project phases, increased user density and geographical coverage.		
WIFI.006	**Functional Requirement**	The Wi-Fi transition from one access point to another shall be seamless. Users must be able to use same login details even if they move from one Wi-Fi zone to another.		
WIFI.007	**Functional Requirement**	The Wi-Fi transition from one access point to another shall be seamless. Users must be able to use same login details even if they move from one Wi-Fi zone to another.		
WIFI.008	**Functional Requirement**	Advertising streams shall be planned and implemented carefully. Because of the advertising, there shall not be a scenario where the citizen is unable to login to the network for a long time and gets annoyed.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.009	**Functional Requirement**	It is expected that the time taken by the user to login and use the Internet from the time he sees the initial page shall be less than 3 minutes.		
Access Point				
WIFI.010	**Functional Requirement**	For the implementation of a city Wi-Fi network, the following are the types of infrastructure being proposed for Wi-Fi Access Points: • Outdoor Rated Access Points (AP) on Smart Poles; • Outdoor Rated Access Point (AP) co-located on Street Light Pole; • Integrated with Multi-Services Digital Kiosk.		
WIFI.011	**Functional Requirement**	The access points shall be capable of managing and configuring remotely through a wireless controller.		
WIFI.012	**Functional Requirement**	The access points shall be capable of managing and configuring remotely through a wireless controller.		
WIFI.013	**Functional Requirement**	Wi-Fi access point shall support dual frequencies (in compliance with DoT and TRAI regulations) including both 2.4 GHz and 5 GHz spectrum. It shall support wireless mesh configuration for redundancy of the network in case of a fibre link being unavailable.		
WIFI.014	**Functional Requirement**	Access points shall support 802.11ac wave II multi-user MIMO.		
WIFI.015	**Functional Requirement**	Access points shall have an integrated in-built or external antenna (IP67).		
WIFI.016	**Functional Requirement**	User can create a profile which will be authenticated using his mobile number (SMS) and email. Further, user can also login using his city application i.e. smart card based session.		
WIFI.017	**Functional Requirement**	Access Point and Multi-Services Digital Kiosks shall be connected using dedicated fibre optic infrastructure for backhaul to Point of Presence (POP).		
WIFI.018	**Functional Requirement**	The Wi-Fi access point shall be controller based that can be managed by using Wi-Fi controller at Control Centre or POP.		
WIFI.019	**Functional Requirement**	The Wi-Fi access point shall be configurable using a Wireless Management system. The software shall include profile configuration, built-in diagnostic, alignment tools, network mapping, network monitoring and maintenance and highly developed security features.		
Wi-Fi Controller				

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.020	**Functional Requirement**	Wi-Fi network shall include Wi-Fi controller to monitor, manage, and control access points from the Control Centre.		
WIFI.021	**Functional Requirement**	The controller shall ensure seamless roaming within city limits.		
WIFI.022	**Functional Requirement**	The controllers should communicate back and forth with the centralized security system and network management system in real time.		
WIFI.023	**Functional Requirement**	The controller shall have inbuilt wireless intrusion protection capabilities		
Wi-Fi Management System				
WIFI.024	**Functional Requirement**	The City-wide Wi-Fi shall also include a Wi-Fi management software and application with a secure login procedure.		
WIFI.025	**Functional Requirement**	The City-wide Wi-Fi shall also include a Wi-Fi management software and application with a secure login procedure.		
WIFI.026	**Functional Requirement**	Wi-Fi management system shall be a centralized system to monitor, analyse, and configure wireless network in automatic fashion. It shall be an authentication and management system for the city Wi-Fi network and shall be installed at the Control Centre or POP.		
WIFI.027	**Functional Requirement**	The system shall be capable of providing Access Point groups with the highest quality network resource allocation by analysing the past 24 hours of RF network statistics, and optimizing the network for the next day.		
WIFI.028	**Functional Requirement**	GUI: The system shall have a configurable graphical user interface (GUI) to provide user friendly experience for policy management, and day to day administration functions.		
WIFI.029	**Functional Requirement**	Database: The system shall have a centralized database and subscriber management system.		
WIFI.030	**Functional Requirement**	The Wi-Fi network shall support multiple BSSIDs as needed to support the overall concept of operations including support for multiple operators.		
WIFI.031	**Functional Requirement**	Fully redundant Authentication, Authorization, and Accounting (AAA) services with OTP/password shall be provided to support city wide services.		
WIFI.032	**Functional Requirement**	The Wi-Fi network shall include a billing software that shall automatically generate the revenue from all the services being offered using this network. This billing software will have transparent interface with Client’s systems.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
User Login Authentication and Plans				
WIFI.033	**Functional Requirement**	Beyond the 30 minutes or 50 MB limit, the user shall have to go through the process of logging in again. At this stage, the MSI may offer custom plans to the users.		
WIFI.034	**Functional Requirement**	Industry standard two (2) step authentication shall be required for all sessions.		
WIFI.035	**Functional Requirement**	iOS and Android applications to be given for seamless connectivity to network-Autodetect/Autologin.		
WIFI.036	**Functional Requirement**	The user shall have the option of either logging in by viewing advertising or can obtain a coupon for the session for a nominal cost.		
WIFI.037	**Functional Requirement**	Premium plans shall be offered to the users on daily, weekly or monthly subscriptions basis. Also, there shall be plans for the residential or industrial users who can pay a small premium to use their dwelling Wi-Fi service across the city.		
WIFI.038	**Functional Requirement**	Users shall have an option to enable/ disable connection to city Wi-Fi.		
WIFI.039	**Functional Requirement**	Users shall also get prompts and alerts for excess data usage.		
WIFI.040	**Functional Requirement**	Multiple payment gateway integration required allowing the users to make the payments using online/ offline mode, including prepaid mobile balance & e-wallet applications and coupon based.		
WIFI.041	**Functional Requirement**	Client shall be able to generate MIS report to view overall usage, collections and other usage statistics over a defined time period.		
Encryption and Security				
WIFI.042	**Functional Requirement**	The Wi-Fi network shall have built-in encryption mechanism to encrypt all communications and data transfer over the Wi-Fi for all the users of Wi-Fi.		
WIFI.043	**Functional Requirement**	Wi-Fi network shall not connect to rogue networks. It shall be segmented for public and utility networks by using VPNs or separate networks in the wired core so that any traffic from the Internet users is not routed into any other sensor network and vice-versa.		
WIFI.044	**Functional Requirement**	Wi-Fi network shall support Protected Extensible Authentication Protocol (PEAP) protocol.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.045	**Functional Requirement**	Wi-Fi network shall have a wireless network content filtering tool for filtering of malicious content on the internet such as pornography sites, rogue sites, torrents etc.		
WIFI.046	**Functional Requirement**	The Wi-Fi Network shall support industry standard two step authentication for secure login procedure.		
WIFI.047	**Functional Requirement**	The Wi-Fi Network shall allow users to roam securely from one access point to another, within or across subnets, without any perceptible delay security during re-association.		
WIFI.048	**Functional Requirement**	The Wi-Fi Network shall support BSSID based IEEE 802.1X authentication and accounting.		
WIFI.049	**Functional Requirement**	The Wi-Fi network shall support MAC based authentication to provide simple authentication based on users MAC address.		
TECHNICAL REQUIREMENTS				
General				
WIFI.050	**Technical Requirement**	The Wi-Fi central hardware and software shall be installed at the POP or Control Centre.		
WIFI.051	**Technical Requirement**	• Organization IEEE: -IEEE 802.11a/b/g/n/ac • Organization European Standard (EN) • Organization Underwriters Laboratory and IEC • Department of Telecommunications guidelines • Telecom Regulatory Authority of India guidelines		
Access Point				
WIFI.052	**Technical Requirement**	The Wi-Fi access point shall be Outdoor rated, dual radio, 802.11ac Wave II, 5-GHz and 2.4-GHz. It shall support operations in 802.11a/b/g/n/ac.		
WIFI.053	**Technical Requirement**	The Wi-Fi access point shall be supplied with MIMO sectoral (120x30 degrees) or omni-directional antennas (in-built or external) as needed to meet the design requirements of the Project. It shall support multiple unique antenna patterns. The antennas shall have antenna gain required to support the coverage requirements of the Project.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.054	**Technical Requirement**	The Wi-Fi access point shall have a built-in spectrum analyser capable of part-time or dedicated spectrum analysis through the provided solution to identify sources of RF interference.		
WIFI.055	**Technical Requirement**	The Wi-Fi access point shall be controller based that can be managed by using Wi-Fi controller at Control Centre /POP.		
WIFI.056	**Technical Requirement**	The Wi-Fi access point shall be configurable using a Wireless Management system. The software shall include profile configuration, built-in diagnostic, alignment tools, network mapping, network monitoring and maintenance and highly developed security features.		
WIFI.057	**Technical Requirement**	The Wi-Fi access point shall provide the fastest and highest throughput with lowest latency even in the most challenging RF environment.		
WIFI.058	**Technical Requirement**	The Wi-Fi access point shall support dual frequency as authorized by DoT.		
WIFI.059	**Technical Requirement**	The total transmitted power (EIRP) of the Wi-Fi access points shall be in compliance with the regulations of the Department of Telecom (DoT), India.		
WIFI.060	**Technical Requirement**	The Wi-Fi access point shall have multiple SSIDs with QoS and security policies.		
WIFI.061	**Technical Requirement**	The Wi-Fi access point shall allow setting up of configurable speeds per user and configurable number of users. It shall support up to 100 concurrent users at any time.		
WIFI.062	**Technical Requirement**	The Wi-Fi access point shall support reliable multicast video to maintain video quality.		
WIFI.063	**Technical Requirement**	The Wi-Fi access point shall also support additional features for Client’s staff members as needed using a separate secure SSID. Each AP shall support at least 16 different BSSIDs.		
WIFI.064	**Technical Requirement**	The Wi-Fi access point shall be IEEE 802.3af/at Power over Ethernet (POE)/POE+ compliant.		
WIFI.065	**Technical Requirement**	The Wi-Fi access point shall support: • Minimum One PoE+ autosensing port 10/100/1000BASE-T Ethernet network interface (RJ-45) and one SFP/SFP+ for fiber connectivity (optional). • Power over Ethernet or Power over Ethernet+.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.066	**Technical Requirement**	The Wi-Fi access point shall have LED based visual indicator for: • Power/System status • Link status		
WIFI.067	**Technical Requirement**	The Wi-Fi access point shall be capable of working at a temperature range of 0˚C to 55˚C and at a humidity of 5% to 95%, non-condensing.		
WIFI.068	**Technical Requirement**	The Wi-Fi access point shall be IP67 compliant or NEMA 4X rated.		
WIFI.069	**Technical Requirement**	The Wi-Fi access point must support IPV4 and IPV6.		
WIFI.070	**Technical Requirement**	The Wi-Fi access point shall support telnet and/or SSH login/ console for troubleshooting.		
WIFI.071	**Technical Requirement**	The Wi-Fi access point shall be reliable ensuring fast, dependable bandwidth and industry standard encryption for security.		
WIFI.072	**Technical Requirement**	The Wi-Fi access point shall independently be configurable to handle security, mesh, RF Management, QoS, roaming, local forwarding without the need for a controller so as to increase performance of the WLAN network.		
WIFI.073	**Technical Requirement**	The Wi-Fi access point shall be supplied with OEM mounting kit and shall support pole mounting option for locations on street light poles or smart poles.		
Wi-Fi Controller				
WIFI.074	**Technical Requirement**	The controller shall support 802.11a/b/g/n/ac.		
WIFI.075	**Technical Requirement**	Each controller shall support at least 500 access point nodes at a minimum and shall be scalable as and when required up to 2000 access points per controller.		
WIFI.076	**Technical Requirement**	The Controller shall support redundancy feature i.e. Active: Active and Active: Standby features. Same licence shall be shared by the controllers.		
WIFI.077	**Technical Requirement**	The controller shall ensure a high throughput even in the most challenging RF environment.		
WIFI.078	**Technical Requirement**	The controller shall be highly available with minimum downtime.		
WIFI.079	**Technical Requirement**	The controller shall ensure seamless roaming.		
WIFI.080	**Technical Requirement**	The controller shall have inbuilt wireless intrusion protection capabilities.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.081	**Technical Requirement**	The controller shall have ability to map SSID to VLAN and it shall ensure VLAN reliability by proactively determining and adjusting to changing RF conditions.		
WIFI.082	**Technical Requirement**	The controller shall support user load balancing to balance the number of users across multiple APs to optimize AP and user throughput.		
WIFI.083	**Technical Requirement**	The controller shall be capable of managing authentication, encryption, IPv4 and IPv6 Layer 3 services.		
WIFI.084	**Technical Requirement**	The controller shall have hot swappable redundant power supplies to maintain uninterrupted network operations.		
WIFI.085	**Technical Requirement**	The controller shall meet the following power specifications: • AC input voltage: 100 VAC to 240 VAC • AC input frequency: 50-60 Hz		
WIFI.086	**Technical Requirement**	The controller shall meet the following environmental specifications: • Operating temperature range: 5°C to 40°C • Operating humidity of 10% to 90% non-condensing		
WIFI.087	**Technical Requirement**	The Wi-Fi controller shall be reliable ensuring fast, dependable bandwidth and industry standard encryption for security.		
WIFI.088	**Technical Requirement**	The controllers shall support two (2) dual-media ports: 2 x 10 Gigabit Ethernet interface or more.		
WIFI.089	**Technical Requirement**	The controller shall be rack mountable.		
WIFI.090	**Technical Requirement**	The controller shall support 1+1, 1+N, and N+N backup configurations.		
WIFI.091	**Technical Requirement**	The controller shall support synchronization of 802.1X state information and wireless client’s 802.11 information from master to backup controller.		
WIFI.092	**Technical Requirement**	The controller shall support minimum 250 VLANs.		
WIFI.093	**Technical Requirement**	The controller shall support airtime fairness feature to ensure equal RF transmission time for wireless clients.		
WIFI.094	**Technical Requirement**	The controller shall support web-based authentication to provide a browser-based environment to authenticate clients that do not support the IEEE 802.1X supplicant.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.095	**Technical Requirement**	The controller shall support AES or TKIP encryption to secure the data integrity of wireless traffic		
Wi-Fi Management System				
WIFI.096	**Technical Requirement**	Wi-Fi management system shall be a centralized system to monitor, analyse, and configure wireless network in automatic fashion. It shall be an authentication and management system for the city Wi-Fi network and shall be installed at the Control Centre. It shall support plug-and-play environment with zero configuration.		
WIFI.097	**Technical Requirement**	GUI: The system shall have a configurable graphical user interface (GUI) to provide user friendly experience for policy management, and day to day administration functions.		
WIFI.098	**Technical Requirement**	Database: The system shall have a centralized database and subscriber management system.		
WIFI.099	**Technical Requirement**	The system shall be capable of providing Access Point groups with the highest quality network resource allocation by analysing the past 24 hours of RF network statistics, and proactively optimizing the network for the next day.		
WIFI.100	**Technical Requirement**	It shall be integrated with tool for monitoring and managing radio frequency (RF) dynamics within the wireless network, to include the following functions and benefits: • Accurate location information for all wireless users and devices • Up-to-date heat maps and channel maps for RF diagnostics • Visual display of errors and alerts		
WIFI.101	**Technical Requirement**	The system shall be capable of restricting bandwidth to a user/users as per the policies.		
WIFI.102	**Technical Requirement**	The system shall be both IPv4 and IPv6 compliant.		
WIFI.103	**Technical Requirement**	The system shall be capable of logging and creating real time reports for users per access point and controller the bandwidth usage.		
WIFI.104	**Technical Requirement**	The system shall be capable of displaying a list of managed devices and access points associated to the Wi-Fi controller.		

Sr. No.	Parameter	Minimum Requirement Description Compliance	Compliance (Yes/No)	Deviations/ Remarks
WIFI.105	**Technical Requirement**	Subscriber services: The system shall provide the users with a self-service portal to enable the new users to register, subscribe, seek information on tariff and billing, update user profile, and make payment through the portal.		
WIFI.106	**Technical Requirement**	The system shall support SNMPv3, SSHv2 and SSL/SSH for secure management.		
WIFI.107	**Technical Requirement**	The system shall support AP grouping to enable administrator to easily apply AP-based or radio-based configurations to all the APs in the same group.		
WIFI.108	**Technical Requirement**	The system shall support selective firmware upgrade APs, typically to a group of APs minimize the impact of up-gradation.		

Annexure 7: Digital display and kiosk

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city 's weather conditions MSI should access and provision for 24*7 operation)

7.1 Outdoor Digital Display Specifications

Sr.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/ Remarks
DSN.REQ.001	LED Type	SMD		
DSN.REQ.002	Best Viewing Distance(m)	> 10 Meter		
DSN.REQ.003	Pixel Pitch	8/6/5 mm as per location requirement		
DSN.REQ.004	Pixel Density	>15000 Dots/m2		
DSN.REQ.005	Brightness	>= 6000 cd/m2 (Adjustable) or better		
DSN.REQ.006	Refresh Frequency	>= 1000 Hz (Adjustable)		
DSN.REQ.007	MTBF	> 10,000 Hours		
DSN.REQ.008	Max Power Consumption	800 Watt/ m2		
DSN.REQ.009	Average Power Consumption	260 Watt/ m2		
DSN.REQ.010	Viewing Angle	140° Horizontally & 45°Vertically		
DSN.REQ.011	Color	>=68 Billion @ 16 bit Processing depth		
DSN.REQ.012	Color Temperature	R.G.B brightness 256 level adjustable		
DSN.REQ.013	IP Rating	IP 65 Front & IP 54 Rear		
DSN.REQ.014	Life Span	> 100000 Hours (After that 50 % Illumination)		
DSN.REQ.016	Operating Temperature	0 ° C to 55° C		
DSN.REQ.017	Operating Humidity	10 % RH to 90% RH		
DSN.REQ.018	OS Platform	Windows 7/ 10		
DSN.REQ.019	Communication Interface	RJ45 (if required, bidder needs to provide media convertor for direct fiber termination)		
DSN.REQ.020	Certification	CE, FCC, UL/ETL/CB		
DSN.REQ.021	Software Display Controller	· Should be able to remotely configure and manage at least 100 LED Screen from a Central location · Should be able to play the selective contents at different LED Screens as per the requirement · Should provide an easy-to-use playlist format for scheduling of content, images, videos, live feeds such as weather forecasts or the news, social media etc. · Assign roles and permissions to allow multiple content		

Sr.No	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/ Remarks
		creators and managers · Should have an interface for content design with readymade/custom made templates · Should have options for importing video feeds, Images and contents from other sources such as inputs from Environmental Sensors, Social Media, Camera Feeds etc. · The Hardware for the central Display Controller has to be provided along with the proposed solution · From the scalability point of view, the software should be able to do so without any extra Licensing up to 200 LED Screens		

7.2 Location and sizes of Outdoor Digital Displays

S. No	Location	No. of Panels	Size	Base Height of Installation
1	Airport	4	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
2	Railway station	2	(2057 mm/81"/6.75') x (2743 mm /108"/9')	18'
3	Central Bus stand	1	(2057 mm/81"/6.75') x (2743 mm /108"/9')	18'
4	Prozone Mall (North gate)	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
5	Bibi ka Maqbara	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
6	Panchakki	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
7	Collector Office	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
8	CIDCO Bus stand	1	(2057 mm/81"/6.75') x (2743 mm /108"/9')	18'
9	Shivaji Museum	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
10	Bharat Mata Mandir	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
11	ASCDCL Head office Main Lobby- AMC HO	1	(2057 mm/81"/6.75') x (2743 mm /108"/9')	18'
12	Dr. Babasaheb Ambedkar Reasearch Centre	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
13	Maulana Abul Kalam Azad Research Centre at Majnu Hill	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
14	Near Kranti Chowk	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
15	Nirala Bazar- Golden Mile	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
16	Cannought Place	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
17	University Bamu Administrative Building	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
18	Divisional Commisioner Office	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
19	Police Commissioner office	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
20	Siddharth Garden	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
21	Gulmandi	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
22	Usnmanpura (Sant Eknath Natyghuha)	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
23	Garkheda	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
24	TV Centre	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
25	Shahgunj	1	(1372mm/54"/4.5') x (1829 mm/72"/6')	12'
	Total	**30**		

7.3Indoor touch Kiosks

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/Remark
Kiosk001	Touch Technology	PCAP (TouchPro® Projected Capacitive) - 12 Touch		
Kiosk002	Diagonal Size	42'' diagonal, Active matrix TFT LCD (LED))		
Kiosk003	Aspect Ratio	16:9		
Kiosk004	Active Area (mm)	36.62" x 20.06" / 930.24mm x 523.26mm minimum or better		
Kiosk005	Resolution	1920 x 1080 @ 60hz		
Kiosk006	Viewing Angle	Horizontal: ±89° or 178° total / Vertical: ±89° or 178° total		
Kiosk007	Number of Colors	16.7 million		
Kiosk008	Brightness (typical)	PCAP: 430 nits		
Kiosk009	Response Time-total (typical)	8 msec		
Kiosk010	Contrast Ratio	4000:1		
Kiosk011	I/O Ports	Input: AC power input, USB type B (for Touch), VGA, 2x HDMI,GPIO, DisplayPort, Audio Line in Output: Audio Headphones out, RJ45		
Kiosk012	Input Voltage	100-240VAC, 50/60Hz		
Kiosk013	Power Consumption (Typical)	(Typical at 230V at 50Hz): ON: 80.0 W SLEEP: 7.0 W OFF: 2.1 W		
Kiosk014	Regulatory approvals and declarations	BIS,CE		
Kiosk015	Mounting Options	VESA mount per MIS-F, 400, 400, 6MM		
Kiosk016	MTBF	50,000 hours demonstrated		
Kiosk017	Computing Module			

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/Remark
Kiosk018	Processor	Qualcomm Snapdragon APQ8053 2.0GHz Octa-Core Processor or better		
Kiosk019	Memory (RAM)	2GB DDR3L		
Kiosk020	Storage	16GB SSD		
Kiosk021	I/O Ports	HDMI output, 2x USB 2.0 Ports, MicroSD card slot, Ethernet 1x LAN (Gigabit), GPIO		
Kiosk022	Control Buttons	Power, Home		
Kiosk023	Wireless	802.11 b/g/n/ac		
Kiosk024	Bluetooth	Bluetooth 4.1		
Kiosk025	OS	Android 7.1/windows		
Kiosk026	Power Supply	AC input voltage: 100-240 VAC Input frequency: 50-60 Hz		
Kiosk027	Power Consumption (Typical)	ON: 4.2W OFF: 3.8W SLEEP: 0.12W or better		
Kiosk028	Dimensions	6.50" x 5.34" x 0.94" / 165 mm x 136 mm x 24 mm		
Kiosk029	Operating Temperature	As per location in aurangabad		
Kiosk030	Regulatory approvals and declarations	BIS,UL, FCC (US)		
	Analytics			
Kiosk031	CPU Monitoring	Monitor any device’s CPU usage in real time. Track user activity to ensure your content reaches your audience.		
Kiosk032	Device Status	Receive notifications regarding device health. If a device goes offline, you’ll be be the first to know about it.		
Kiosk033	Now Playing	View active screenshots of the content currently playing on your devices.		

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/Remark
Kiosk034	Location	Track the placement of all your devices on an interactive map		
Kiosk035	Alerts and Timlines	Monitors device alerts and sends notification emails based on the severity of the issue.		
	Remote Management			
Kiosk036	Device Settings	the power to adjust your device's settings such as volume and brightness.		
Kiosk037	Software Update	Remotely update your devices as new software updates become available.		
Kiosk038	Data Reset	Restore your device to factory defaults, and wipe any locally-stored content.		
Kiosk039	Data Logs	Collect data logs of your device activity		
Kiosk040	Device Reboot	can be remotely rebooted from the 'Device Settings' page.		
Kiosk041	Device Orientation	Switch between portrait and landscape mode on your devices		
Kiosk042	Filters	Use parameter based search to quickly locate specific devices in your device list.		
Kiosk043	Remote Network Proxy configuration	Provides ability to setup Network Settings and Proxy configuration on a device		
Kiosk044	Whitelisting of Apps	Ability to whitelist Apps on a device		
	Device Grouping			
Kiosk045	Drag and Drop	Add devices to a group by dragging and dropping the device into a group.		
Kiosk046	Group Settings	Easily adjust the settings of an entire group. Group changes affect all devices within the group.		

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/Remark
Kiosk047	Device Search	Manage your device library with ease. Use keywords to quickly locate a specific device or group.		
Kiosk048	OS	Automated deployment of latest OS image and content		
Kiosk049	API	Over-the-air updates (triggered from the device or an API)		
	Kiosk Enclosure Specifications			
Kiosk050	Enclosure Specifications	Enclosure shall be made of Sheet metal and shall be IP 66 rated.		
Kiosk051	Metal specifications	Housing shall be made in a minimum 16 gauge that should be powder coated as per the required colour choice.		

7.4Indoor Non touch Kiosks

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/ Remark
KioskNT001	Diagonal Size	42'' diagonal, Active matrix TFT LCD (LED))		
KioskNT002	Aspect Ratio	16:9		
KioskNT003	Active Area (mm)	36.62" x 20.06" / 930.24mm x 523.26mm		
KioskNT004	Resolution	1920 x 1080 @ 60hz		
KioskNT005	Viewing Angle	Horizontal: ±89° or 178° total / Vertical: ±89° or 178° total		
KioskNT006	Number of Colors	16.7 million		
KioskNT007	Brightness (typical)	500 Nits		
KioskNT008	Response Time-total (typical)	8 msec		
KioskNT009	Contrast Ratio	4000:1		
KioskNT010	I/O Ports	Input: AC power input, USB type B (for Touch), VGA, 2x HDMI,GPIO, DisplayPort, Audio Line in Output: Audio Headphones out, RJ45		
KioskNT011	Input Voltage	100-240VAC, 50/60Hz		
KioskNT012	Input Connector	IEC 60320 C6		
KioskNT013	Power Consumption (Typical)	(Typical at 230V at 50Hz): ON: 80.0 W SLEEP: 7.0 W OFF: 2.1 W		
KioskNT014	Regulatory approvals and declarations	BIS,UL, FCC (US)		
KioskNT015	MTBF	50,000 hours demonstrated		
	Computing Module			
KioskNT016	Processor	Qualcomm Snapdragon APQ8053 2.0GHz Octa-Core Processor Or Better		
KioskNT017	Memory (RAM)	2GB DDR3L		
KioskNT018	Storage	16GB SSD		

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/ Remark
KioskNT019	I/O Ports	HDMI output, 2x USB 2.0 Ports, MicroSD card slot, Ethernet 1x LAN (Gigabit), GPIO		
KioskNT020	Control Buttons	Power, Home		
KioskNT021	Wireless	802.11 b/g/n/ac		
KioskNT022	Bluetooth	Bluetooth 4.1		
KioskNT023	OS	Android 7.1/Windows		
KioskNT024	Power Supply	AC input voltage: 100-240 VAC Input frequency: 50-60 Hz		
KioskNT025	Power Consumption (Typical)	ON: 4.2W OFF: 3.8W SLEEP: 0.12W		
KioskNT026	Dimensions	6.50" x 5.34" x 0.94" / 165 mm x 136 mm x 24 mm		
KioskNT027	Regulatory approvals and declarations	BIS,CE		
	Analytics			
KioskNT028	CPU Monitoring	Monitor any device’s CPU usage in real time. Track user activity to ensure your content reaches your audience.		
KioskNT029	Device Status	Receive notifications regarding device health. If a device goes offline, you’ll be be the first to know about it.		
KioskNT030	Now Playing	View active screenshots of the content currently playing on your devices.		
KioskNT031	Location	Track the placement of all your devices on an interactive map		
KioskNT032	Alerts and Timlines	Monitors device alerts and sends notification emails based on the severity of the issue.		
	Remote Management			
KioskNT033	Device Settings	the power to adjust your device’s settings such as volume and brightness.		

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations/ Remark
KioskNT034	Software Update	Remotely update your devices as new software updates become available.		
KioskNT035	Data Reset	Restore your device to factory defaults, and wipe any locally-stored content.		
KioskNT036	Data Logs	Collect data logs of your device activity		
KioskNT037	Device Reboot	can be remotely rebooted from the 'Device Settings' page.		
KioskNT038	Device Orientation	Switch between portrait and landscape mode on your devices		
KioskNT039	Filters	Use parameter based search to quickly locate specific devices in your device list.		
KioskNT040	Remote Network Proxy configuration	Provides ability to setup Network Settings and Proxy configuration on a device		
KioskNT041	Whitelisting of Apps	Ability to whitelist Apps on a device		
	Device Grouping			
KioskNT042	Drag and Drop	Add devices to a group by dragging and dropping the device into a group.		
KioskNT043	Group Settings	Easily adjust the settings of an entire group. Group changes affect all devices within the group.		
KioskNT044	Device Search	Manage your device library with ease. Use keywords to quickly locate a specific device or group.		
KioskNT045	OS	Automated deployment of latest OS image and content		
KioskNT046	API	Over-the-air updates (triggered from the device or an API)		
	Kiosk Enclosure Specifications			
KioskNT047	Enclosure Specifications	Enclosure shall be made of Sheet metal and shall be IP 66 rated.		
KioskNT048	Metal specifications	Housing shall be made in a minimum 16 gauge that should be powder coated as per the required colour choice.		

Annexure 8: ICT Enabled Solid Waste Management

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

8.1RF ID TAG

Sr.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/ Remarks
RFID01	Power	Tags should be passive. RFID tags should be rewritable. It should allow writing of information like vehicle number, contractor details etc.		
RFID02	Operating Frequency	865-868MHz		
RFID03	Data Transfer Rate	At least 512 kbps under ideal conditions & 64 to 512 kbps under field conditions		
RFID04	Tag Id	Unique Id given by a chip manufacturer (64 bits or 8 bytes)		
		EPC Gen 2, ISO 18000-6C		
RFID06	Dimensions (including the substrate/ backing)	Maximum area occupied on the windshield shall be 50 Sq. cm.		
RFID07	Material	Plastic substrate with printed antenna		
RFID08	Physical printing of Tag ID on the Tag	The Tag ID shall be physically printed on the Tag using the Hexadecimal numbering system and shall be adequately clear for easy visual recognition		
		The RFID Tag shall be installed at a fixed location on the inside of the Windshield of the vehicle. (location to be optimized for each class of vehicle during testing)		
		The RFID Tag shall have a self-adhesive backing with which it can be fixed to inside of the windshield. The adhesive shall be such that		
RFID09	Location & Installation	It allows reliable and accurate reading of the Tag by the Transceiver located at a specified distance.		
		The RFID chip and/ or the antenna get irreparably damaged when an attempt is made to remove the installed Tag from the windshield by any means. After such an attempt the Tag shall become inoperable.		
		Unique Tag ID – 64 bits, EPC memory – 240 bits		
RFID010	Tag Memory (Minimum)	Unique Tag ID -64 bits, EPC memory -240 bits		
RFID011	Data Retention	10 Years minimum with UV protection for normal sunlight exposure and ambient temperature of 45 Degree Celsius		

8.2 RF ID Metal Tag

Sr.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
RFIDM01	Chip Type	1. UHF Class 1 Gen 2		
		2. EPC 96 bit extendable up to 480 bits		
		3. User Memory 512 bit		
		4. Data retention of 50 years		
		5. Write endurance 100,000 cycles		
RFIDM02	Operating Frequency	865-868MHz		
RFIDM03	Operating Range	6 to 10 meters when mounted on Metallic surface		
RFIDM04	Operating mode	Passive (battery-less transponder)		
		-20°C to +85°C		
RFIDM07	Ingress Protection	IP 66		
		Rugged construction for high durability with Screw holes for mounting with Screws on a metallic surface		

8.3 Bin Sensor

Sr.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
BS01	Enclosure	Polypropylene		
BS02	Shape & Dimension	Cubical shape with max size of 100mmX80mmX50mm Or Mushroom shaped with max diameter of 100 mm & height		
BS03	Weight	Up to 450 gm		
BS04	Enclosure Protection	IP 67		
		-20 C to + 80 C		
BS06	Power Supply	High performance battery		
BS07	Battery Life time	Approximately 5 years		
BS08	Built In Modem	GSM modem/shield for 2G or 3 G communication		
BS09	Level Sensor	Ultrasonic sensor with IP rating		
BS010	Range	0.2 meter to 4 meters		

8.4 Boomer Barrier

S.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations/Remarks
BB1	Supply Voltage	110V AC or 220V AC		
BB 2	Boom Material	Aluminium Alloy		
		Cast Iron		
BB 3	Ingress Protection	IP 54		
B 4	Barrier Length	5 - 5.8 m		

8.5 Hand Held Bio Metrix Device

S.No.	Parameter	Minimum Specifications or better	Compliance (YES/NO_	Deviations /Remarks
BMH1	Communication	1 - 2G/3G GPRS Data & SMS		
BMH 2		2 - WiFi with IEEE 802.11 a/b/e		
BMH 3		3 - Ethernet LAN 100 Base-T		
BMH4		4- Inbuilt GPS		
		All options are mandatory and required		
BMH 5	Display	128×64 pixel LCD, white LED backlight and specific icon		
BMH 6	Fingerprint reader (Optical Fingerprint Scanner of ANSI and ISO formats)	High Performance Optical Sensor (500dpi),with large capture area ,Must have 1:1 authentication and 1:N identification		
BMH 7	Inbuilt Card Reader	Inbuilt Card Reader for Mifare classic, Ultralight, DESFire, ISO 14443 A & B & SONY FeliCa or 1 wire protocol		
		2.8 inch or higher TFT LCD		
		16 or more Keys rubber rugged alphanumeric keypad		
BMH 8	Processor & Memory	32-bit ARM11 400MHz or better CPU with minimum 64MB RAM & 128MB FLASH		
		Rechargeable Li-on Battery 2600mAH or more with minimum 12 hours of user operations		
		Firmware must be upgradeable over the air from central location, there shall be no need to physically connect device to computer to upgrade the firmware		
BMH 9	Device certification	CE, RoHS, EMV4.3 Level 1 & 2 ISO9001 & ISO14001 for Manufacturer		
BMH 10		-Provide Manufacturer Authorization Certificate certifying the bidder/supplier		
BMH11	Central User management (including centralized Biometric Registration)	User registration shall happen centrally including biometric captures, using desktop computers, the data shall be then pushed to all/selected remote devices over internet		
BMH 12	Software Source code	Source code related to Device and Central Software (if any), shall be submitted to tendering authority, Source code ownership will be transferred to tendering authority with complete documentation.		

8.6 Weighbridge 40 MT Capacity

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations /Remark
WB001	Load-Cells	'Double Ended Shear Beam' or 'Compression Type Capacity: 30 mt of each 8m,9m& 12m platfarm size 4/6 nos. and for 16000 x 3000 & 18000 x 3000 mm platfarm 6/8 nos. will be supplied.		
WB002	Nominal Load / Rated Capa.	Each Load cell capacity 20/30 Tonnes.		
WB003	Max. Load without damage to Load Cell (Safe Load)	150% of Rated Capacity		
WB004	Destructive load/	300% Rated Capacity		
WB005	Ultimate rated output	3.0 mv/V		
WB006	Combined Error	<0.02% of rated capacity		
WB007	Repeatability	< +/-0.01% Full Scale output.		
WB008	Hysteresis Error	< +/-0.02% FSO		
WB009	Excitation Voltage	10 V DC –Max. 15 VDC		
WB010	Environmental Protection	IP-68		
WB011	Temperature Compensated Range	0 degree to 60 degree		
WB012	Humidity	100% RH(Max.)		
WB013	Creep (30 minutes)	< +/-0.03% FSO		
WB014	Insulation Resistance	>1000 Meg Ohms at 50VDC		

Sr.nos	Item	Minimum Requirement Discription	Complaince (yes/No)	Deviations /Remark
WB015	Allowed Side Load	50% of rated capacity		
WB016	Side Load Discrimination	500:01:00		
WB017	Non Linearity	< +/-0.025% FSO		
WB018	Zero Balance	< +/- 1.0% FSO		
WB019	Input Resistance	770 +/- 20.0 Ohms		
WB020	Input Resistance	700 +/- 7.0 Ohms		
WB021	Temp. Effect on output	< +/- 0.0015% FSO/ Deg. C		
WB022	Temperature effect on Zero	< +/- 0.0020% FSO/ Deg. C		
WB023	Deflection	< 0.5 mm at FSO		
WB024	Finish and Construction	Electroless Nickel Plated Tool Steel		

Annexure 9: Aurangabad Citizen Mobile Application and Website

(* The specifications provided in this RFP are indicative minimum and carry guiding rule. The MSI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards, govt Guidelines compliances & best practices adopted in the industry) subject to approval from ASCDCL)

(Operating temperature where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

(Power backup where ever applicable should be as per Aurangabad city ‘s weather conditions MSI should access and provision for 24*7 operation)

Annexure 10– Locations

10.1 CCTV Camera

Note: All locations and the camera numbers are indicative. The final number and the locations shall be confirmed to the successful bidder.

Sr. no	Locations	Police Station	PTZ	Fixed
1	Aurangpura Chowk (Mahatma Phule Chowk)	City Chowk		2
2	Aurangpura Bhajimandi			1
3	Bhadkal Gate			2
4	MaNaPa Tea			1
5	City Chowk			1
6	Gandhi Statue			2
7	Shahgunj Chaman		1	1
8	Barabhai Tajiya			2
9	Gulmandi Parking			2
11	Supari Hanuman Mandir Chowk (Front Side)			1
12	Hudco Corner			1
13	Chelipura Chowk		1	1
14	Uddhavrao Patil Chowk			1
14	Annabhau Sathe Chowk		1	1
15	Jubliee Park		1	1
16	Collector Office / Strike Point		1	2
17	Jama Masjid			1
18	Hotel Taj			1
19	Kumbharwada / Mahavir Bhavan			1
20	Maharashtra Hindi College			
	Chowk			3
21	Sarafa Line			1
22	Road to Kumbharwada			2
23	Aurangabad Book Depot			1
24	Delhi Gate			1
25	Div Commissioner Office Tea			
	Point / Strike Point		1	2
26	Kileark			1
27	Road to Bhaji Mandi (Pathakphoto Chowk)			2
29	Anjali Theatre Chowk (Road to Khadkeshwar Temple)		1	2
30	Chaitanya Gorkshnath Chowk, Nageshwarwadi			1
31	Nageshwarwadi Y Point			1
32	Pandaribaba Chowk			1

Sr. no	Locations	Police Station	PTZ	Fixed
33	Shah Bazar			1
34	Old Bazar Chowk			1
35	Road from Kasari Bazar / VIP Bag			1
36	Hindi Collage Tea Point			1
37	Multipurpose high school Tea Point			1
38	Salim Ali Sarovar and Majnuhill Garden Area			2
39	Marathwada Sanskritik Sports Mandal Chowk			1
40	Rangargalli			1
41	Kasari Bazar			1
42	Kirana Chawdi Chowk			1
43	Front of Murmura Masjid			1
44	Manjurpura Chowk			1
45	Mohan Theatre			1
46	Bohri Kathada			1
47	Sansthan Ganpati Chowk		1	2
48	Road form Kasari Bazar/VIP Bag			1
49	Hindi Collage Tea Point			1
50	Kala Darwaja			1
51	D Mart Mall			1
52	Navjivan Colony Kaman			1
53	Annabhau Sathe Chowk Siddhart Nagar			1
54	Bidhi LaneJajira Hotel			1
55	Kamakshi Chowk		1	1
56	City Chowk Police Station			1
57	Front of Municipal Corporation Office			2
58	Sille Khana Chowk		1	2
59	Nirala Bazar		1	1
60	Paithan Gate		1	2
61	Ulhaq Jim (Zone 1 Office)		1	2
62	BSNL Chowk / Maharishi Walmiki Chowk	Kranti Chowk	1	2
63	Satish Motors Tea Point			1
64	Below Kranti Chowk Flyover		2	3
65	Above Kranti Chowk Flyover			1
66	Amarprit Chowk		1	2
67	Below Mondha Naka Flyover		1	2
68	Above Mondha Naka Flyover			1
69	Road to Aurangpura Visarjan Well South Road		1	1
70	Baburao Kale Chowk, Nirala Bazar			2
71	Savarkar Chowk			2

Sr. no	Locations	Police Station	PTZ	Fixed
72	Aurangpura Police Station		1	1
73	Nath Super Market Aurangpura			1
74	Mill Corner		1	2
75	Bustand (Parking / Garden / Hotwater)		2	1
76	Kartiki Chowk		1	1
77	Baba Petrol Pump (Below / Above)			3
78	Roxy Theatre Tea Point			1
79	Law Collage Hostel Frontside/ Road to Samarth Nagar			1
80	Shriman Shrimati			1
81	Jafar Gate Chowk			1
82	Banjara Colony			1
83	Samata Nagar Chowk			1
84	Saraswati Bhuvan Bus Stop		1	1
85	Ajab Nagar Tea Point			1
86	Rama Nagar Tea Point			1
87	Rokadiya Hanuman Tea Point			1
88	Shivsena Bhavan Chowk			1
89	Nutan Colony Tea Point			1
90	Shivaji HighSchool			1
91	Bandu Vaidya Chowk / Police			
	Socity Office Chowk			1
92	Varad Ganesh Front Side			1
93	ST Div Office			1
94	Kokanwadi Chowk (Ahilyabai			
	Holkar Chowk)		1	2
95	Vits Hotel			1
96	Railway Staion IN/OUT Gate	Vedant Nagar	1	2
97	Bridge of Railway station			
	Above			2
98	Panchvati Chowk			2
99	Bansilal Nagar Tea Point			1
100	Sneh Nagar Tea Point /SSC Board			1
101	Ram Mandir Padampura			1
102	RTO Office			2
103	Govt Treasury Road			1
104	Road to Vedant Nagar Police Station		1	1
105	Govt Polytechic Front Side			1
106	Session Court		1	2
107	Near Walking Plaza			1
108	Below Railway Station Bridge/ Two Points			2
109	Chunnilal Petrol Pump/Near Water Tank			1

Sr. no	Locations	Police Station	PTZ	Fixed
110	MTDC Front Side			1
111	Railway Station MIDC road Front road of Deogiri Collage			1
112	Front of Dhoot Motors			1
113	Front of Deogiri Collage			1
114	Ayodhyanagri Ground			1
115	Railway Station Parking / Internal Area			1
116	Nagar Naka	Chawni	1	2
117	Lokhandi Bridge			1
118	Panchakki Gate / Malik Ambar Chowk		1	1
119	Barapulla Gate			1
120	Milind Chowk			1
121	Nehru Chowk Rajasthan Hotel			1
122	Bhaji Mandi			1
123	PES Collage T / Law Collage Chowk			2
124	Nandvan Colony			2
125	Patel Chowk			2
126	Deluxe Bakrey			1
127	Shantipura Chowk			1
128	Mahatma Phule chowk ground			1
129	Mauli Medical			1
130	MaNaPa Hospital Chowk			1
131	Dr.Ambedkar Chowk			1
132	Amin Chowk			1
133	Railway Over Bridge (Nagar Road)			1
134	Gawlipura Corner Chowk			1
135	Private Bus Parking in Baba			
	Petrol Pump Chowk			1
136	Shahkar Nagar Colony Chowk			1
137	HDFC ATM Chowk			1
138	Daulatabad Tea Point			2
139	Tarangan Tea Point			1
140	Kadri Hospital			1
141	Padhegaon Chowk			2
142	Walmiki Chowk			1
143	Sant Tukaram Maharaj Mandir			1
144	Raje Sambhaji Chowk			1
145	Near Mugdiya Plotting			1
146	Ramgopal Nagar			1
147	Machindranath Mandir			1
148	Milind Collage Gate			1
149	Firebut Road			1
150	Priyadarshani Colony			1

Sr. no	Locations	Police Station	PTZ	Fixed
151	Road Chawni Police Station			1
152	MEBT Point			1
153	Militry Office Canteen Tea			
	Point			1
154	Income Tax Office Tea Point			1
155	Garampani Bridge/Chawni			
	Bazar Ghati Hospital		1	2
156	Gate/OPD/Accident Department/Medical Collage/New Medicine Building			4
157	Begumpura Chowk			1
158	University Gate		1	1
159	Lal Masjid		1	1
160	Bibi Ka Makbara		1	1
161	Subhedari Tea Point		1	2
162	Below Townhall Bridge			2
163	Makai Gate	Begumpura		1
164	Begumpura Smashanbhoomi Tea Point			1
165	Amkhas Ground		1	2
166	TB Hospital Chowk			1
167	Cancer Hospital			1
168	Above Townhall bridge			1
169	Police Commissioner Office			3
170	Dr.Babasaheb Statue Y Junction		1	2
171	Choti Masjid Turn Point			1
172	Main Gate of Buddha Cave/Area of Buddha Cave			1
173	Statue in Botenical Garden			1
174	Asefiya Colony			1
175	Cave Tea Point (Hanuman Tekdi)			1
176	Administrative Building of University Frontside			2
177	Soneri Mahal			1
178	Kulguru Residance Chowk (Natyagruh/Sai)			1
179	Makaigate Pragati Colony			1
180	Ghati Employees Quartars			
	Road			1
181	Road to Begumpura Police Station			1
182	Champa Chowk		1	2
183	Roshan Gate			2
184	Rammandir,Kiradpura			2
185	Central Naka Chowk	Jinsi	1	2
186	Azad Chowk			2

Sr. no	Locations	Police Station	PTZ	Fixed
187	Akashwani Chowk		1	3
188	Seven Hill		1	2
189	Jinsi Chowk		1	2
190	Bagga Hotel			1
191	Near RC Bafna Chowk/To Apex Hospital			1
192	Apex Hospital Tea			1
193	Bayjipura Chowk			2
194	Old Mondha Area			3
195	Laxman Chawdi Chowk/Kailas Nagar,Road to Sanjay Nagar			2
196	Road to Madni Chowk			1
197	Kaphatiya Hospital Road			1
198	Hotel Silver Inn Galli			1
199	Road to Khas Gate			1
200	SuranaNagar			1
201	Motiwala Nagar			1
202	Khas Gate			1
203	Bayjipura Masjid			1
204	Nijamoddin Chowk/Road from Champa Chowk			1
205	Honda Showroom / Natural Icecream			1
206	Kasture Galli			1
207	Ahinsa Nagar			2
208	Kalda Corner		1	2
209	Gopal Tea			1
210	Sant Eknath Mandir Chowk			1
211	Gadhe Chowk		1	1
212	Bhajiwali Bai Putla Chowk			2
213	Utsav Chowk		1	2
214	Dargha Chowk		1	2
215	Jyoti Nagar Chowk			1
216	Pratap Nagar Tea/Near Gurukrupa Teeth Hospital			2
217	Chausar Chowk	Usmanpura		1
218	Chota Murlidhar Chowk/MIDC Quartars			1
219	Pirbazar Chowk			2
220	Sathe Chowk			1
221	Mitra Mandal Society Chowk			1
222	Shrey Nagar Chowk			1
223	Zambad Estate			
	Chowk/Deogiri Bank			1
224	Road to Jabinda Estate to			

Sr. no	Locations	Police Station	PTZ	Fixed
	Pratap Nagar			1
225	Dashmesh Nagar			1
226	Kailash Fastfood/Bansod			
	Classes Chowk			2
227	Dwarkapuri/Pratap Nagar			1
228	Road from Railyway station MIDC Gate			1
229	Road to Rama Nagar			1
230	Agnihotri Chowk/Max Hospital T			1
231	Trimurti Chowk		1	2
232	Jawahar Nagar Chowk			1
233	Front of Patel Complex Near Jawahar Nagar Police Station			1
234	Police Station Jawahar Nagar Chowk	Jawahar Nagar	1	2
235	Ulkanagri Ramayana Hall Chowk			2
236	Below Sangram Nagar Flyover			2
237	Above Flyover			2
238	Roplekar Chowk		1	1
239	Gajanan Maharaj Mandir Chowk		1	3
240	Hedgewar Hospital Chowk/Mehersingh Naik Chowk			3
241	Front of Janki Hotel			2
242	Adinath Chowk			2
243	Easy Day/Bazar Tal/Private			
	Bus Station			2
244	Gurudwara Kaman			1
245	Radhakrishana Managal Karyalay Chowk		1	1
246	Ulkanagri Corner Chowk			1
247	Chetak Ghoda Chowk			2
248	Garkheda Chowk/Sutgirni Chowk		1	2
249	Road to Deputy Mayor			
	Residance			1
250	Sigma Hospital T			1
251	Sahakar Nagar Chowk			2
252	Near Water Tank of Shivaji Nagar		1	2
253	Deshpande Puram			1
254	Khivansara Park			2
255	Gadiya Vihar		1	1
256	Front of Chaurangi Hotel Chowk			2
257	MSEB Power Station(Indra Nagar Slum area)			1
258	Maruti Mandir Garkheda Chowk			1
259	Trisharan Chowk			1
260	Ambedkar Chowk		1	2

Sr. no	Locations	Police Station	PTZ	Fixed
261	Wokhardt T		1	1
262	N-1 Chowk			1
263	Cidco Bus Stand		1	1
264	SBI Bank Corner			1
265	Jalgaon T		1	3
266	Deogiri Bank Chowk/Wokhardt T			1
267	Rama Hotel Gate/High court Gate	CIDCO		1
268	Ramgiri Chowk			1
269	Jalgaon T above Flyover			1
270	TV Center Chowk		1	2
271	Savarkar Chowk IP mess			2
272	Venutai Chavan high school corner			1
273	Zone 2 Office Chowk/ Jakat Naka			2
274	Maniyar Chowk			1
275	Cannaught T/Cannaught Total Area/Shiva Hotel		1	4
276	Chistiya Chowk		1	2
277	Baliram Chowk			2
278	Onkar Gas Chowk			1
279	Avishkar Chowk			1
280	Jijau Chowk,N-11		1	1
281	Saptrshungi Chowk			1
282	Road to N-6 Near Renuka mata mandir			1
283	Front of Laxmi Tel Bhandar TV Centre			1
284	Sant Tukaram Natyagruh N-5			2
285	M-2 Farshi Maidan T			1
286	Sona Mata Highschool L Sector			1
287	Garware Chowk			1
288	Ambassador Chowk			1
289	MGM Gate/ MGM Area			1
290	Road to MGM			1
291	Bajrang Chowk		1	2
292	Maharashtra Bank Chowk			1
293	Fornt of SP Office			1
294	Green Park hotel T			1
295	MaNaPa School T			1
296	Renukamata Mandir N-9			1
297	Deogiri Bank Stop			1
298	Bharat Mata Chowk Police Colony N-10			1
299	Misarwadi Gaon			1
300	Shivaji Putla Behind Cidco Post			1
301	Indian Airlines T			1

Sr. no	Locations	Police Station	PTZ	Fixed
302	Ranaji Mangal Karyalay			1
303	Yashwant Housing Society			1
304	Front of Laxmi Provision			1
305	Front of MaNaPa Hospital			1
306	Front of Dwarkadas Shamkumar Shop			1
307	MGM Gate			1
308	Parshwanath Chowk			1
309	Savangi Chowk	Harsul		1
310	Harsul Gaon			2
311	Jatwada T Point/Jail Area			2
312	Harsul Tea Point		1	3
313	SBOA Chowk		1	1
314	Sai Medical T			2
315	Saubhagya T			2
316	Sharad T Point		1	3
317	Tulja Bhavani Chowk/Mayur Park Road			2
316	Mhasoba Mandir Mhasoba Nagar			1
317	N-11 Navjivan Colony Shopping Center			1
318	Maruti Mandir Mayur Park		1	1
319	Harsul Gaon Dr. Ambedkar Putla/Maruti Mandir			1
320	N-11 Navjivan Colony Buddha Vihar/Hanuman Mandir			1
321	Front of New Highschool			1
322	Bhagatsingh Nagar Chowk			1
323	Harsiddhi Mata Mandir Area			1
324	Chatrapati Sambhaji Chowk			1
325	Pisadevi Gaon Chowk			1
326	Bhaji Market Mondha			1
327	Jadhavwadi Dhanya Market and Internal Area			2
328	Office of Vijay Autade			2
329	Mohini Rajpuram chowk			1
330	Godavari T		1	2
331	Mahanubhav Ashram		1	2
332	Link road Tea Point			2
333	MINAZ HOTEL			1
334	Kamalnayan Bajaj Hospital/Sudhakar Nagar Road			1
335	MIT Chowk			2
336	Satara Khanodba Mandir Back Side			2
337	Satara Khanodba Mandir Front Side	Satara		1

Sr. no	Locations	Police Station	PTZ	Fixed
338	IRB Y Point			1
339	Ekta Hotel Chowk Satara Gaon			2
340	Deolai Chowk		1	2
341	Chatrapati Nagar Beed Bypass			1
342	Nath Vally School Chowk		1	1
343	Best Price Chowk Paithan Road			1
344	Nirlep Company Chowk			2
345	Vitkheda T			2
346	Shahshokta Durga road Bypass T			2
347	Road to Satara Post			2
348	Nishant Park Hotel Tpoint (Atharv Chowk)		1	1
349	Renukamata Kaman			1
350	Chatrapati Shau Maharaj			
	Sanstha Chowk			1
351	Jabinda Lawns Jain international Chowk			1
352	Santaji Chowki			1
353	Riverdale School Chowk			1
354	Road to Naiknagar			1
355	Devanagri Railway Gate			1
356	Satara Police Station		1	
357	Near Mahavir Chowk Police Station			2
358	Deva Nagari			1
359	Barhale Hospital Chowk			1
360	Sudhakar Nagar T			1
361	Front of Marathwada Garrage Beed Byepass			1
362	Front of Pagariya Showroom Beed Bypass road			1
363	Sai Mandir Near Chate School			1
364	Ayappa Mandir road			2
365	Datta Mandir Beed road			1
366	Mauli Nagar T			1
367	ST Workshop Chowk		1	2
368	Dhoot Hospital Chowk			2
369	Airport IN/OUT Gate			1
370	Govt Hospital Chikalthana		1	1
	Shukrawar Bazar Chikalthana			2
371	Cambridge Naka		1	1
372	Maharashtra Distilary			1
373	GGT Chowk		1	1
374	M Cidco Police Station Front			1
375	NRB Chowk	M CIDCO		1
376	Prozon Mall Gate T		1	2

Sr. no	Locations	Police Station	PTZ	Fixed
377	Airport Parking/Passanger Entry Gate/Area		1	2
378	Chikalthana Gaon			1
379	Nagarsevak Raju shinde Kaman			1
380	Hanuman Chowk			2
381	Old Jalna Naka		1	1
382	East Side road to Chikalthana Gaon to beed Road/Old Airport Runway nearby road		1	1
383	Bridgewadi Gaon		1	2
384	Dharamkata/M Cidco Police Station Front			1
385	Front of M Codco Police Station		1	1
386	Kamgar Chowk N-3 Cidco		1	2
387	Area of Mukundwadi Railway Station		1	3
388	API Corner		1	2
389	Mukundwadi Shivaji Putla			1
390	BharatMata Railway Crossing		1	1
391	Thakare Nagar N-2 Chowk		1	1
392	Jai Bhavani Nagar Chowk		1	2
393	Road to Cidco Flyover/Road	Mukundwadi		
	from Flyover			1
394	Ram Nagar Kaman/Internal Area			1
395	Maa Saheb Chowk			1
396	Lahuji Salve Chowk		1	1
397	Naregaon Chowk			1
398	Naregaon		1	3
399	Savangi Byepass road/Naregaon T		1	2
400	Guru Lawns Beed Bye Pass			1
401	Road to N-2 Stadium			1
402	BharatMata Railway Crossing		1	1
403	Mahalaxmi Chowk			1
404	Ambika Nagar Chowk N-2			1
405	Fornt of Buddha vihar Jaibhavani Nagar			1
406	Guru Lawns Beed Byepass			1
407	High Court East North Road		1	1
410	Front of HighCourt Quarters			1
411	Sanjay Nagar Dr.Babasaheb Ambedkar Putla			1
412	Balasaheb Chowk		1	1
413	Mukundwadi Gaon Maruti Mandir			1
414	Old Jakat Naka(Road to Chikalthana Gaon)			1

Sr. no	Locations	Police Station	PTZ	Fixed
415	Iwan Hotel Chowk/Mukundwadi Police Station Road			1
416	Pilot Baba Nagar			2
417	Jai Bhavani Nagar Galli No 1,2,3			1
418	Sanjay Nagar Kaman/Internal Area			1
419	President Park / Garware Stedium			2
420	Kalagram			2
421	Kasliwal Corner			1
422	Near Gokul Sweet Mart			1
423	Pundlik Nagar Chowk Shivaji Statue			1
424	Railway Gate No-56 /Raj Nagar		1	2
425	Chatrapati Collage Gate			2
426	Akshay Deep Complex N-4	Pundlik Nagar		1
427	Hindu Rashtra Chowk			2
428	Reliance Mall Chowk		1	1
429	Vijay Nagar Chowk			1
430	Wani Mangal Karyalay Chowk			2
431	N-4 Chowk Nagre's Residance Front Side			1
432	MIT Hospital Chowk, N-4		1	2
433	Front of Patiyala Bank			2
434	Hanuman Nagar Chowk			1
435	Essar Petrol Pump			1
436	Parijat Nagar			1
437	Bharat Nagar/Beside Railway Line			2
438	Mahadeo Mandir N-3			1
439	Area of Adinath Nagar			2
440	Pundlik Nagar Railway Line Slum Area		1	2
441	Abhinay Chowk			1
442	Moti Karanja chowk			1
443	Raja Bazar			1
444	Aurangpura Bus stand			1
445	Aurangpura Bhaji market			
446	Darga Chowk			1
447	Champa Chowk			1
	Total		**100**	**600**

10.2 Digital Display Signages

Sr.No.	Location	No. of Panels
1	Airport	4
2	Railway station	2
3	Central Bus stand	1
4	Prozone Mall (North gate)	1
5	Bibi ka Maqbara	1
6	Panchakki	1
7	Collector Office	1
8	CIDCO Bus stand	1
9	Shivaji Museum	1
10	Bharat Mata Mandir	1
11	ASCDCL Head office Main Lobby- AMC HO	1
12	Dr. Babasaheb Ambedkar Research Centre	1
13	Maulana Abul Kalam Azad Research Centre at Majnu Hill	1
14	Near Kranti Chowk	1
15	Nirala Bazar- Golden Mile	1
16	Cannought Place	1
17	University Bamu Administrative Building	1
18	Divisional Commisioner Office	1
19	Police Commissioner office	1
20	Siddharth Garden	1
21	Gulmandi	1
22	Usnmanpura (Sant Eknath Natyghuha)	1
23	Garkheda	1
24	TV Centre	1
25	Shahgunj	1

Note: The locations mentioned here are indicative. ASCDCL shall confirm the final location to the successful bidder.

10.3 Wi-Fi Hotspots

Sr	Locations	Estimated User Count during Peak Hours	No. of Wifi Hotspots	Level	Nos of AP	access point
1	AMC Head Office + Post Office	700	4	H	10	40
2	Gulmandi	1000	5	H	10	50
3	Niralabaar	800	4	H	10	40
4	High Court + News Paper Office Road	550	3	M	5	15
5	Shivaji Nagar	600	3	M	5	15
6	Sidhardth Gardan	600	3	L	2	6
7	Bajaj Hospital	600	3	L	2	6
8	MGM / JNEC	700	4	H	10	40
9	Gajanan Maharaj Mandir / Hedgevar Hospital	800	4	M	5	20
10	Canought Place	800	4	H	10	40
11	Central Bus Stand	850	5	H	10	50
12	Railway Station	900	5	H	10	50
13	Prozone Mall	1000	5	H	10	50
14	Kamgar Chowk	650	4	L	2	8
15	Garkheda	600	3	M	5	15
16	Amarpreet Hotel	550	3	L	2	6
17	Kranti Chowk	800	4	M	5	20
18	Usmanpura / Gopal Tea	750	4	H	10	40
19	Kalda Corner	650	4	M	5	20
20	Dhooth Hospital	600	3	L	2	6
21	Bibi ka Makbara	550	3	L	2	6
22	Panchakki	650	4	H	10	40
23	Collector Office / Divisional Commissioner Office	800	4	M	5	20
24	Maulana Azad College	650	4	H	10	40
25	IHM	500	3	H	10	30
26	Harsool T Point	650	4	H	10	40
27	IJTR	650	4	H	10	40
28	Cidco Bus Stand	700	4	M	5	20
29	Raja Bazaar	750	4	L	2	8
30	HUDCO Corner	550	3	L	2	6
31	TV Center	1000	5	H	10	50
32	Sawarkar Chowk / Samarth Nagar	650	4	M	5	20
33	Roshan Gate	600	3	M	5	15
34	Dr. Babashaeb Ambedkar Marathwada University	600	3	M	5	15
35	Azad Chowk	650	4	M	5	20
36	Chelipura Chowk	550	3	L	2	6
37	Shanur Miya Darga	650	4	M	5	20
38	Bajrang Chowk	600	3	M	5	15

Sr	Locations	Estimated User Count during Peak Hours	No. of Wifi Hotspots	Level	Nos of AP	access point
39	Baba Petrol Pump	1200	6	H	10	60
40	Aurangpura	800	4	H	10	40
41	Shah Bazaar Chowk (Champa Chowk)	400	2	M	5	10
42	Majnoo Hill	600	3	M	5	15
43	City Chowk Police Station	800	4	H	10	40
44	Mahanubhav Ashram	600	3	M	5	15
45	Baijapur – Jinsi Police Station	400	2	M	5	10
46	Shahganj (near Chaman Square)	400	2	M	5	10
47	Saraswati Bhavan School	600	3	H	10	30
		32050	172		Total	1178

10.4 Smart Bus Stops - Location

S.no	Name	X	Y
1	Ambassador Ajanta Hotel Coner	75.361148	19.874865
2	Sutgirni chowk	75.345974	19.859179
3	Opp Naik College	75.364193	19.874548
4	Opp.PVR	75.377497	19.872413
5	Jawahar College	75.34896	19.864856
6	Railway station RTO	75.310219	19.860795
7	Shivajinagar	75.351197	19.853378
8	Gajanan Mandir	75.350926	19.869287
9	Central Bus stand	75.317065	19.880452
10	Shahagunj	75.317275	19.882524
11	Aurangpura ZP	75.32681	19.884145
12	Aurangpura Shishu Vihar	75.326316	19.883271
13	Aurangpura Hostel	75.325737	19.881529
14	Aurangpura SB	75.322759	19.874385
15	Gajanan Mandir road, Jinsi Police station	75.342171	19.884987
16	N1 corner	75.365451	19.879981
17	fame tapadia	75.366168	19.877646
18	Opp SBH Zonal office	75.366196	19.876851
19	CIDCO bus stand	75.366405	19.875706
20	Baba station road	75.314106	19.872666
21	Baba CBS Road	75.317156	19.876495
22	Baba jalna road	75.317005	19.873676
23	LIC	75.317418	19.873581
24	Opp Manmandir new court	75.320574	19.872718
25	ABC Complex	75.320872	19.872613
26	Opp satish Motors	75.322893	19.872281
27	Sahakar bank	75.328663	19.873835
28	Kranti chowk darga	75.328718	19.873206
29	Doodh Dairy	75.331255	19.874336
30	Kranti chowk zone	75.331478	19.874428
31	Sinchan Bhavan	75.342583	19.876168
32	Akashwani	75.344346	19.876411
33	SFS	75.347875	19.876221
34	Seven hill	75.353566	19.875228
35	Opp. Lokmat	75.357481	19.874971
36	Rama International Hotel gate	75.358551	19.874981
37	Sahyadri Hotel	75.359673	19.875003

10.6 Biometrics

Sr. Nos	Item	Location	Qty
1	Finger Print Device		
		Building 1Main Entrance	3
		Building 1Wing 1 Staircase & Parking Entrance	2
		Building 2Wing 2 Staircase & Mayor Area Entrance	2
		Building 3Main, Parking, Closed & Store Entrance	5
		Ward Offices x 9Front & Rear Entrance	18
2	Handheld Finger Print device	Supervisor	50

Annexure 11: Use cases (Systems should be compatible and scalable for Phase 2 Use Cases)

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
1	**Solid Waste Management**	CCC&OCC dashboard will display & monitor the KPIs set along with other information related to waste management if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1) Total Bins in City
			2) Total Bins Full
			3)Total %Bins full in Zone
			4) No. of KPI Violations in last 24 Hr
			5) No. of KPI violations in last XX days
			6) Total vehicles available and movement of each Garbage pick up vehicles/tricycles/handcart on the city map
			7)Total vehicles Faulty
			8)View waste related grievances on the city map as per custom time scale connected to the solid waste management app/web site
2	**Wi-fi Hotspots**	CCC&OCC dashboard will display & monitor the KPIs set along with other information related to Wi-fi management if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1) Total Hotspots across city
			2) Total Online Hotspots
			3) Total Offline Hotspots
			4) Total Users connected
			5) Top 5 websites accessed by users
			6) Total size of Download by users in last 24 Hrs
			7) Total size of Upload by users in last 24 Hrs
			8)cyber attack and suspicious web site access detection
3	City Surveillance System - VMS (Video Management	**Video System Functionalities :-** System CommunicationConnect and authenticateConnect/disconnect	Able to view live and Recorded Video Data from all CCTV cameras, selecting the cameras from the tree or by selecting the cameras from the MAP. Ability to get alert from the video analytics of various types use case mentioned below

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
	Software)**- Safety and Security**	status detectionSensor State Display Alarm Failure TamperOutputs/inputs Dry contactsRelay outputs Video CapabilitiesLive video Playback recorded videoPlayback recorded audio (depends on sub-system)Export live videoExport live audio (depends on sub-system)Export recorded videoExport recorded audio (depends on sub-system)Start/stop recordingPTZ/presetLive video\audio in external monitor (depends on sub-system)Snapshot (depends on sub-system)OSD parametersVirtual toursVirtual tours discoveryLayout discovery (depends on sub-system)External monitors discovery Sensors discoveryVideo favouritesdiscoveryPTZ identification discovery	**Camera Tampering: -** Should make sure cameras are focused on required field of view and any tampering with it create alarm in CCC. For changes in camera Field of View should create alarm For obstructing the camera field of view by too bright or too dark must create alarm
			For Crowd Monitoring inside city Crowd monitoring at sensitive location, if crowd reaches above certain percentage alarm should create in the control room, Also during procession as the crowd start gathering and reaches certain level, these cameras should automatically popup along with alarm and start monitoring from CCC by dragging these cameras on video wall.
			Vehicle Detection: Presence detection for moving and stopped vehicles For vehicle moving in opposite direction, For Vehicle parking in non parking Area Congestion Detection Cameras should create alert for traffic congestions for particular traffic junction.
			.**Abandoned Object Detection**: Object left define- Alert should create in control room Because of background conditions if its difficult to run analytics like left object, in such case operators should able to find trail of abandoned object on all the cameras as part of forensic, immediately after reporting about the object.
			Forensic operator should get access to following data: Recorded and Live Data from Cameras (VMS), Video Analytics Data (Meta Data), Facial Recognition Data , Voice Recording Data- Voice Logger, Operators onscreen activity - Screen Recordings
			Forensic Operator should help in following scenario
			Authenticity of Recorded Data Captured by CCTV cameras through VMS
			Should able to forensic recorded data on selected cameras e.g IN case of alert receive from Face recognition system with current full body photograph of suspect, which will further search on other selected

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
			cameras (Cameras surrounding the FCR camera from alert got generated) on the basis of suspect full body photograph and should able to trace the suspect along with its path on the map.
			Also, should able to reconstruct scenario like call received to control room, action taken by operator and CCTV feeds on site. Post events on single time frame for operator training
			Analysis in CCC would be graphical user interface for search, replay and to simultaneously search and replay recorded telephone systems, GPS data on GIS maps, conventional and digital radio channels as well as trunked radio communications. All communications regarding a specific incident should be replayed together in the sequence in which communications occurred on a synchronised timeline.
			Video Broadcasting: 5 Nos Any camera should able to stream directly to streaming server
4	**Environmental Sensors (Phase-2)**	CCC&OCC dashboard will display & monitor the KPIs set along with other information related to Environmental management if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1) Total count of Environmental Sensors
			2) Total count of ON & OFF
			3) Average Reading of Critical sensors (pollution sensors, noise sensors, particle sensors, Rain Gauge)
			4)View NOX, SO2,co2,O2, Noise, ambient light,humidity,UV levels across the city, view threshold breaches, and view data superimposed on a map. The view should allow the facility to change the time scale
5	**Smart Traffic Management System (Phase-2)**	CCC&OCC dashboard will display & monitor the KPIs set along with other information related to	1) Alert generation for hot listed vehicles like “Stolen”, “Wanted” or any user defined category.2) The ANPR Camera detect and identify the vehicles plying on the wrong lane. The system looks on a lane with a pre-defined

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
		Environmental management if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	direction of motion of the vehicles and as soon as a vehicle is found to be moving in its opposite direction, an alarm is generated.3) This system is capable of detecting Speed of the vehicle at the junction. 4)Man less 24x7 operation5)Integrated e-Challan system can be used for identifying vehicles with unpaid penalties/challans6) It should detect and read license plates automatically in real time and efficiently in night 7)User friendly Graphical User Interface (GUI)8)Detecting Speed of the vehicle,9) Red light violation detection 10)Local junction traffic detection at the intersection11)Also BPM (Business Process Module) in CCC will help to manage and handle the smart Traffic for below scenario Handling VVIP moments - Green Corridor Making Green Corridor - Medical Emergency Applying define traffic control strategies for time of day wise , day wise , or in need basis scenario For all above operator one click able to create event along with relevant mapping such as for VIP moments the VVIP vehicle route on GIS map, and should able to correlate and set parameter to respective assets on the MAP with help of BPM capabilities of CCC, like setting time to intelligent traffic signal for green corridor with intimation on VaMS on these route, displaying all cameras on the route on video wall in CCC
6	**Smart Traffic Management System (TVDS - Traffic Violation Detection System) with ANPR (Phase-2)**		1) Total Violations detected by TVDS
7			1)Total no. of E-challan generated across the city

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
	Smart Traffic Management System (e-Challan System) (Phase-2)	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to Smart Traffic –e-challan system if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	2) Total Value of fine collected across the city through echallan
			Number plates must be captured efficiently in night time
			Detect and read license plates automatically in real time
			Should Integrate with any other module
			Number plates must be captured efficiently in night time as well using IR illuminators
			Integrated e-Challan system can be used for identifying vehicles with unpaid penalties/challans.
8	**Smart Traffic Management System (Public Address System) Phase-2**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to PA Management Solution if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1)total nos of PA system online/offline/ with last massage played
			should play messages as per SOP at particularscenarios, such if traffic jam because of particular vehicle stopping ahead of road crossing etc
9	**Smart Traffic Management System (Variable Message Sign) Phase-2**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to VaMS Management Solution if any KPI is breached a new incident will be reported in CCC&OCC incident management module and	1)Total VaMS across city along with online massage display
			2) Total Online/Offline/Faulty DMS
			3)SOPs base adaptive traffic handling capabilities like displaying traffic congestion action on Variable Messaging Boards, Green Corridor intimation etc.

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
		predefined SOPs will follow for action.	
10	**Smart Transport**	1) Display of GPS enabled vehicles on MAP	1) Nos. of Buses according to routes with Nos. of and KPI Violation like Break Down, Accidents etc.
			Buses running late on the route
			Alert if Buses stop at longer en route
			SOS from Bus Driver should generate alert at control and command center
11	**Smart Parking Management system (Phase-2)**	Displaying Available Parking Slot across city with cameras feed in case of any event.	1) Total count of Parking Slots
			2) Total used Parking slots
			3) Total Available parking slots
			4) Zone wise parking availability status
12	**Smart Pole**	CCC&OCC dashboard will display & Monitor the KPIs set along with other information related Smart Pole management if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1) Poles working
			2) Poles faulty
			3) The cabinet's Electro-magnetic lock which can be open remotely from control and command center.
			4)Alert should be generated in real time in control and command center for open, tamper, power loss etc
			5)Aesthetical Advertisement board provision must available as per sample design guideline s
			6)Pole must be design and installed in such way that it should be weather conditions should not affect or compromise functionality of any equipemnts

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
13	**Video Wall**	CCC&OCC shall integrate the Video wall controlling functions using SDK API so as they can be accessible from CCC&OCC GUI. CCC&OCC GUI shall allow to select any input to any cube/wall, set different inputs on video wall as per requirements.	Video wall must be in operation 24*7. Ergonomically design as per industrial standard for comfortable viewing. Instant viewing change in <2 seconds
14	**SMS/Email Gateway**	CCC&OCC notification engine shall allows sending SMS, email or any such communication using its message templates.	sending email/messages to predefine entity as per SOP from dashboard
15	**GIS Integration**	CCC&OCC dashboard will display & Monitor the KPIs set along with other information related GIS Integration if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	Smart Lighting
			Smart Water
			Smart Transport & Smart Bus Stop
			Smart Traffic (ATMS)
			Smart Parking
			Digital Display Signages
			CCTV based City Surveillance
			IP telephony system along with PA/ECB
			ICT enabled SWM
			Biometric Attendance & IP Telephony System
			E-Governance
			GIS Application
			SMS/e-mail gateway
			Outdoor digital Signage and VaMS (Variable message System)

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
			Able to plot various devices on GIS maps with different layers
			IBMS event and alert
16	**E-Governance Applications (phase-2)**	CCC&OCC dashboard will display & monitor the KPIs set along with other information related to E-Gov management if any KPI is breached a new incident will be reported in C&C incident management module and predefined SOPs will follow for action.	View the aggregate transactions performed at given civic centre on the city map based on data collections from ERP system. Also, its possible to view feeds from ERP system on changing time scale like daily, weekly, monthly, quarterly and yearly.
			Ability to view property tax collected across city area wise with turnaround time of tax collection, selection on MAP with changing time scale like daily, monthly, weekly, quarterly and yearly
			Ability to estimate shortfall of the property tax collected and graphicalrepresentation of same with variable time scale from daily to yearly.
			Ability to view births registered in the city, with classification like Normal /abnormal, the view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly,
			Ability to view turnaround times for issuance of certificate in the city, the view should allow to see the data on changing time scale from daily to yearly basis.
			Ability to view deaths registered in the city, the view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly,
			Ability to view turnaround times for issuance of certificate in the city, the view should allow to see the data on changing time scale from daily to yearly basis.
			View the building permissions (unique view for each license type) issued on the city map. The view should allow the facility to change the time scale from 1 hr. to 1 year, with daily, weekly, monthly, quarterly and yearly views available

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
			View the demand required (water, waste, sewerage, etc.) as a result of building permissions given in the city on the city map.
			View the feeds received from ERP system on the city map.
			Ability to view water related grievances in city, should able to display inputs from SCADA like distribution network, distribution volume and ground utility network also it should able to superimpose on city MAP
			Should ability to view spending pattern across budget heads, area wise budget spent across the city, also various feeds from ERP system. The view should allow the facility to change the time scale from hourly, daily, weekly and yearly views
			Ability to view benefits issues with identification of type of benefits the view should allow the facility to view the data on variable time scale from hourly, daily, weekly, quarterly and yearly.
			Ability to view the project status with type of project, spending on the project with time of award, time of completion.
			Ability to view feeds received from hospital management system with type of diseases noted across city hospitals with
17	**Video Analytics Detection and classification (Phase-2)**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to Video Analytics , if a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	Online Video Analytics event and alert display on the GIS platform, Alert should pop up on the screen with relevant video stream
			1)Behavioural Biometry: Identification through multiple behaviour
			Parking violation
			Speeding vehicle
			Accident detection
			Loitering detection
			Person climbing barricade
			Person collapsing
			Gesture recognition: Identification through gesture change
			Person/Face recognition

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
18	**Artificial intelligence (Overall) Phase-2**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to Artificial Intelligence , if a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1) Graffiti and Vandalism detection2) Debris and Garbage detection3) Attendance of sanitation workers on site by face recognition3) Sweeping and cleaning of streets/bins before and after4)Garbage bin, cleaned or not5)Litter detection6)Tracking of garbage truck movement and Quantity of garbage dumped at dumpsite7)Detection and Recognize the pattern of demonstration and conflicts in crowd8)Detection and classification of human, animal and vehicle
19	**Face Recognition System Multi-Modal Analytics (Phase-2)**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to Face Recognition, if a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	Searches people, vehicles, and moving objects, all under the same user interface.
	Face Recognition System -Source Independence		Provides fast analysis of all video and image data, regardless of the video source.
	Face Recognition System -Post-Event Processing (Phase-2)		Post-event investigations more efficient. For example, it can be used to process video footage captured in the vicinity of an event, like a bombing. Video footage from surveillance cameras, cell phones, and web cams can be input and used to tag items of interest (faces, moving objects, etc.), allowing users to focus their attention on the frames with relevant details, while ignoring the rest. 500 hours of HD video should be pre-processed in 10 hours.
	Face Recognition System -In-Video Matching and		Main matching capabilities: 1) Watch list matching; 2)Person tracking matching. With these two complementary matching capabilities, video

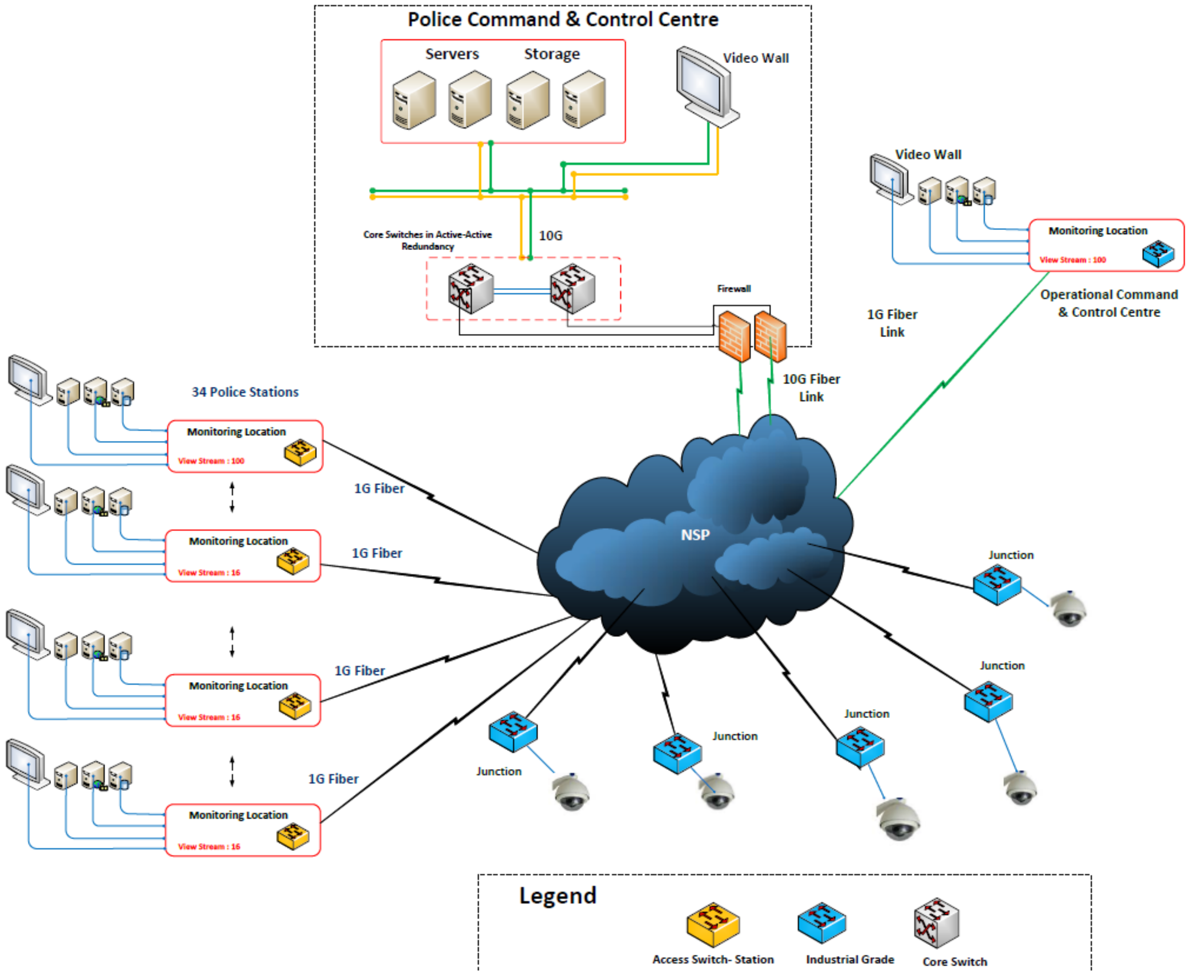
Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
	Grouping (Phase-2)		investigators can build person image groups or records, where all images within a record belong to the same individual. Video investigators can start by entering the images of people who are likely to be involved in the case into a watch list. For each new detection will automatically determine if the detected image corresponds to a watch list entry. Alternatively, investigators can start by selecting an image from the case corresponding to an unknown person and searching it against all other images within the case to find and group all images of that person. In both scenarios, the images within a grouping can be identified by a common tag.
	Face Recognition System - Modalities		Identity & Security algorithms to processes video data and to detect and track: 1) Motion, 2) people by: Silhouette, Face 3) License Plates These modalities can be applied individually or combined, making it a very flexible tool with wide-ranging applications. These modalities are described in the following sub-sections
	Face Recognition System -Motion Detection (Phase-2)		Motion detector algorithm provides the following benefits: 1)Accurately finding moving objects (from a single person riding a bicycle up to a group of consistently moving objects, like people walking together);2) Successfully identifying objects with non-linear trajectories, like people walking in different directions;3)Keeping track with moving objects even when they cross each other;4)Returning the best image of the objects, which means that the:a) Contour of moving objects is found consistently from one frame to the next, the images are tagged, and albums are generated,b)Users can quickly view albums of moving objects.5) Finding moving objects as small as 5 pixels by 5 pixels in the background of the field

Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
			of view;6) Pre-processing objects in motion as a preliminary step before applying other algorithms, making the face or body detection more efficient;7) Eliminating motion “noise”, like the leaves of a tree or when there is wind or rain;8) Supporting both colour and greyscale images
	Face Recognition System -Person detection by Silhouette (Phase-2)		The person detection by silhouette. It is not affected by an individual’s clothing, including hats or scarves. It can find images of people that are at least 60 pixels in height.Silhouette tracking techniques as face and movement trackingSilhouette detection should be on both video and static imagesThe person detection by silhouette function should also detect people who are not standing or walking. Silhouette tracking techniques as face and movement trackingSilhouette detection should be on both video and static images Face detection technology should find faces when there is partial occlusion of the face, low light, and when partially obscured by glasses. face detection and tracking algorithms provide the following benefits:1) No limit to the number of faces that the algorithms can detect and track in a single frame or an image: it can pull all the visible face images in crowded train station.2) Different face detection and tracking strategies can be preset as required to meet your exact needs.3)The algorithm is robust to face orientation changes, up to the limit of where faces can be detected. It can also handle a partial occlusion of the face or short interruptions of the image over time.4) The algorithm recognizes the images of the same person in a video sequence and puts them in an album. Reviewing just the album and not every frame of the video makes the analysis quicker and easier
	face matcher main matching capabilities:		face matcher main matching capabilities:1)Watch List Matching - Matching against images of people of interest within watch lists;2) In-Video Matching - Matching against the face images found within the videos or images submitted Any face found in the videos and photos submitted

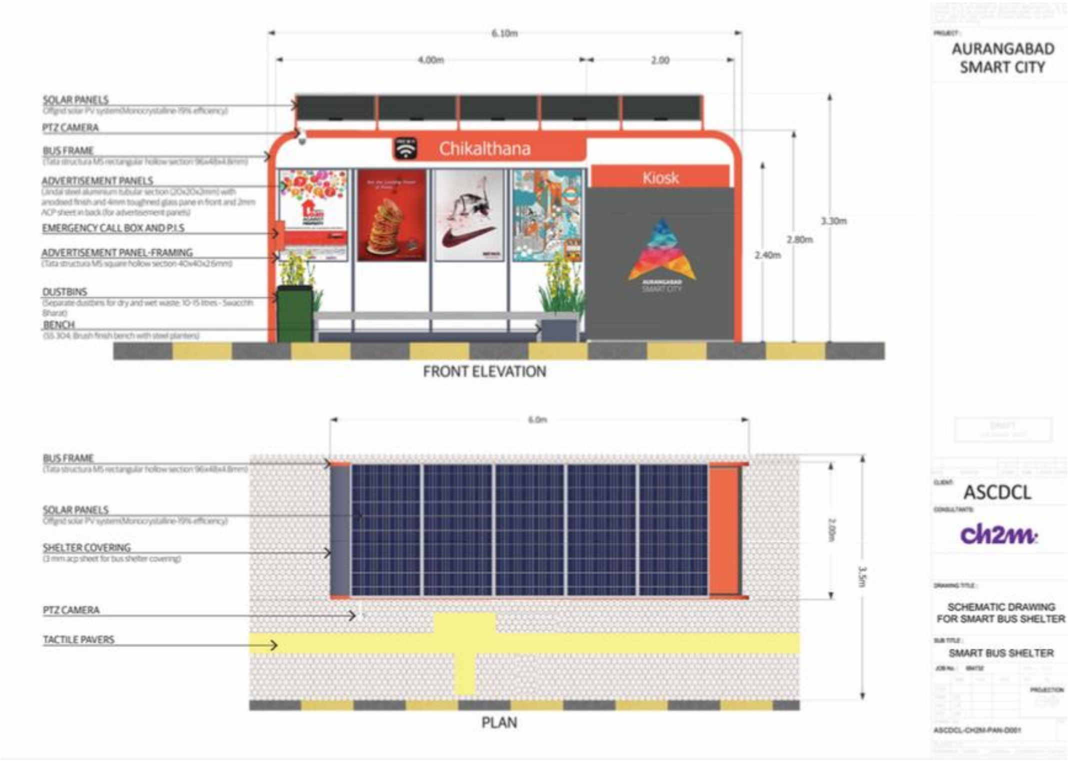
Sr. No.	System	CCC&OCC Integration and Supported Functionalities	Use cases, KPI and Dashboard requirement
			is:3)Compared to images within selected watch lists. Watch list search results are presented in two ways:a)At the detected face level: a specific tag indicates that a detected face is likely to be a match with an individual in a named watch list, allowing the Investigator to confirm the match,b) At the watch list level: the Investigator can review the images of individuals within a watch list has indicated have been seen in submitted videos and photos.4)Written into the matcher.Using this background database, it is possible to compare:a)One or more face images of the same individual against the faces found in the video of the same case (videos and photos are organized by case),b) One or more face images of a suspect (when it is required to know if he or she was visible in the context of a criminal case).Matching of face images extracted from video records may be difficult, as the images are likely to be extremely small, or involve poses, expressions, clothing, or lighting that is far from optimal
20	**Emergency Response Management System (Public Address System, Emergency call box, Camera , IP telephony) (P\\fhase-2)**	CCC&OCC dashboard will display and monitor the KPIs set along with other information related to Emergency Response Management System if any KPI is breached a new incident will be reported in CCC&OCC incident management module and predefined SOPs will follow for action.	1)total nos of PA /ECB system online/offline/ with last massage played 2)In case Emergency if ECB call initiated IP voice/video call must pop up on video wall of CCC and Relevant local Police station with relevant camera stream simultaneously IP call tp be place as per define in SOP 3)Emergency video /voice call to One or multi location as per SOP for the purpose of conference or broadcasting messages 4)Operator from CCC and OCC should able to do play or call from desktop and play defined message ,custom message or announcement to any PA system or group of PA system 5) Head of the department should able to make video/voice call to multiple parties

Annexure 12: Indicative Design

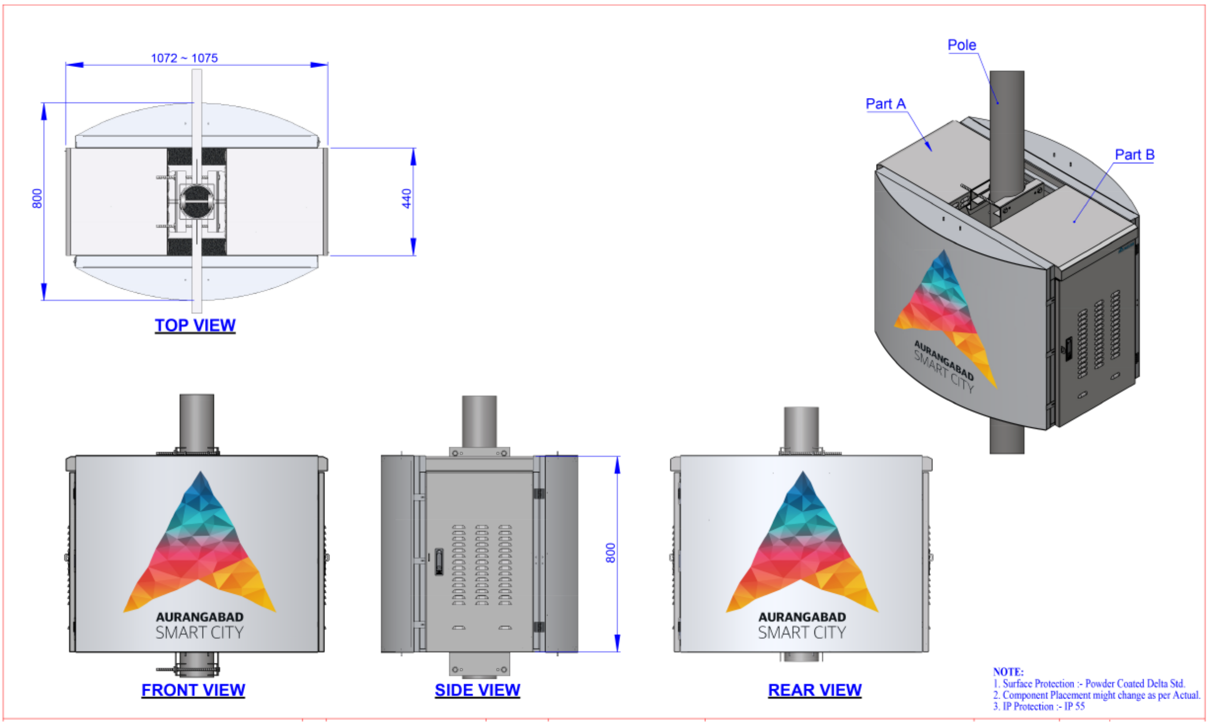
CityNetwork



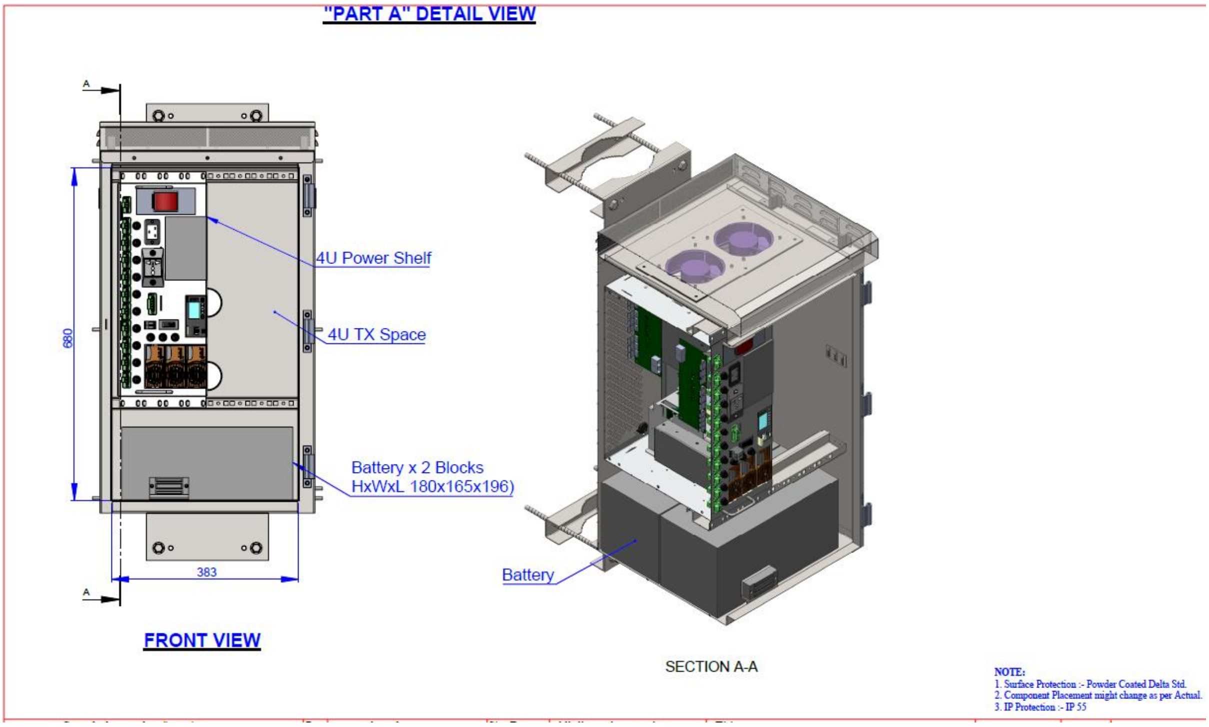
12.1 Sample Design of Smart Bus Stop


6.10m
4.00m
2.00
SOLAR PANELS
Offgrid solar PV system(Monocrystalline 19% efficiency)
PTZ CAMERA
BUS FRAME
(Tata structura MS rectangular hollow section 96x48x4.8mm)
ADVERTISEMENT PANELS
(Jindal steel aluminium tubular section (20x20x2mm) with anodised finish and 4mm toughned glass pane in front and 2mm ACP sheet in back (for advertisement panels)
EMERGENCY CALL BOX AND P.I.S
ADVERTISEMENT PANEL-FRAMING
(Tata structura MS square hollow section 40x40x2.6mm)
DUSTBINS
(Separate dustbins for dry and wet waste, 10-15 litres - Swacchh Bharat)
BENCH
(SS 304. Brush finish bench with steel planters)
Chikalthana
Kiosk
AURANGABAD SMART CITY
2.40m
2.80m
3.30m
FRONT ELEVATION
6.0m
BUS FRAME
(Tata structura MS rectangular hollow section 96x48x4.8mm)
SOLAR PANELS
Offgrid solar PV system(Monocrystalline 19% efficiency)
SHELTER COVERING
(3 mm acp sheet for bus shelter covering)
PTZ CAMERA
TACTILE PAVERS
2.00m
3.5m
PLAN
PROJECT :
AURANGABAD SMART CITY
CLIENT :
ASCDCL
CONSULTANTS :
ch2m
DRAWING TITLE :
SCHEMATIC DRAWING FOR SMART BUS SHELTER
SUB TITLE :
SMART BUS SHELTER
PROJECTION
ASCDCL-CH2M-PAN-D001

12.2 Sample Design of Smart CCTV Pole Junction box

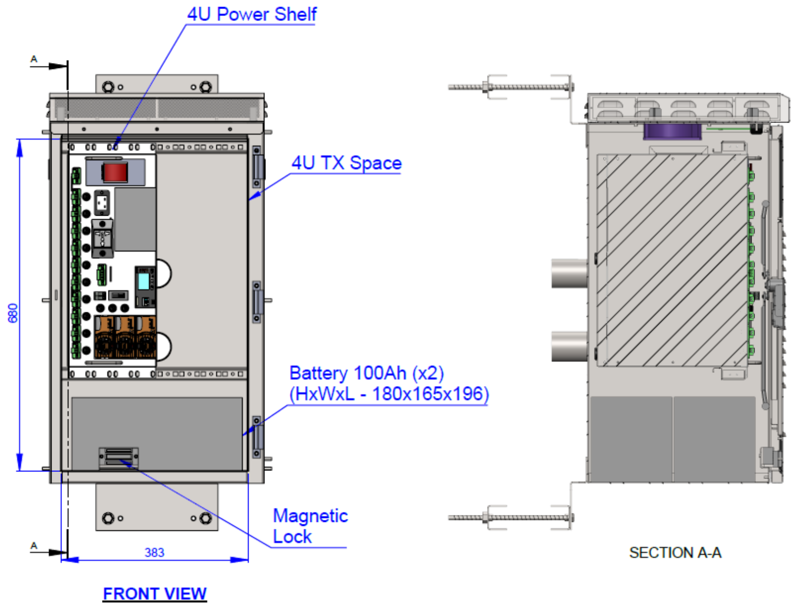


NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55



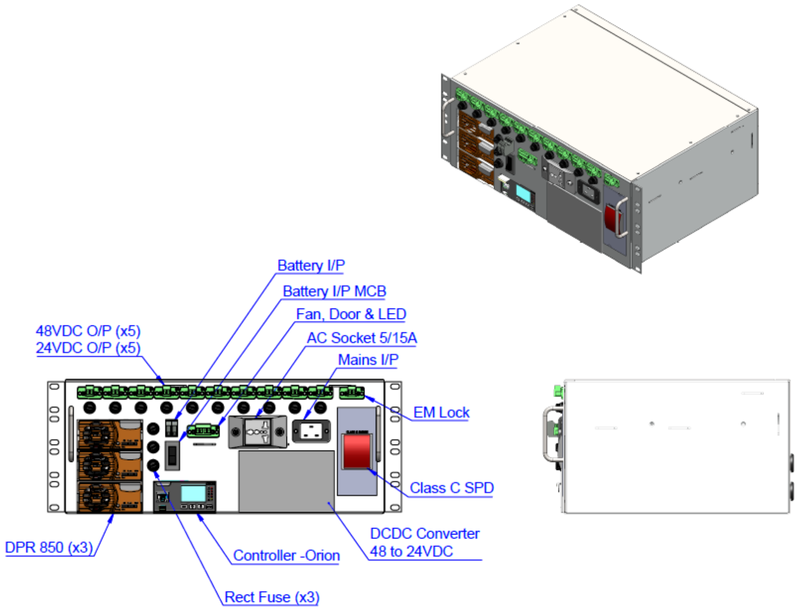
NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55

"PART A" DETAIL VIEW



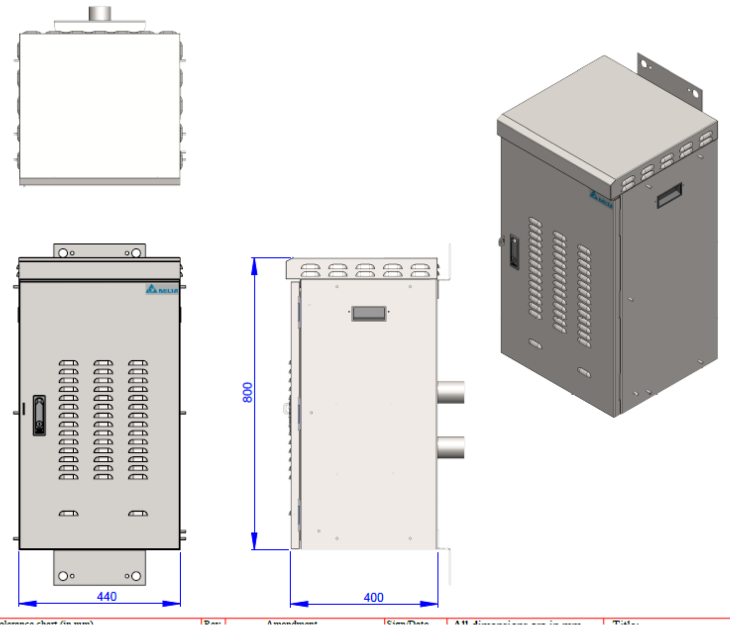
NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55

"PART A" 4U POWER SHELF



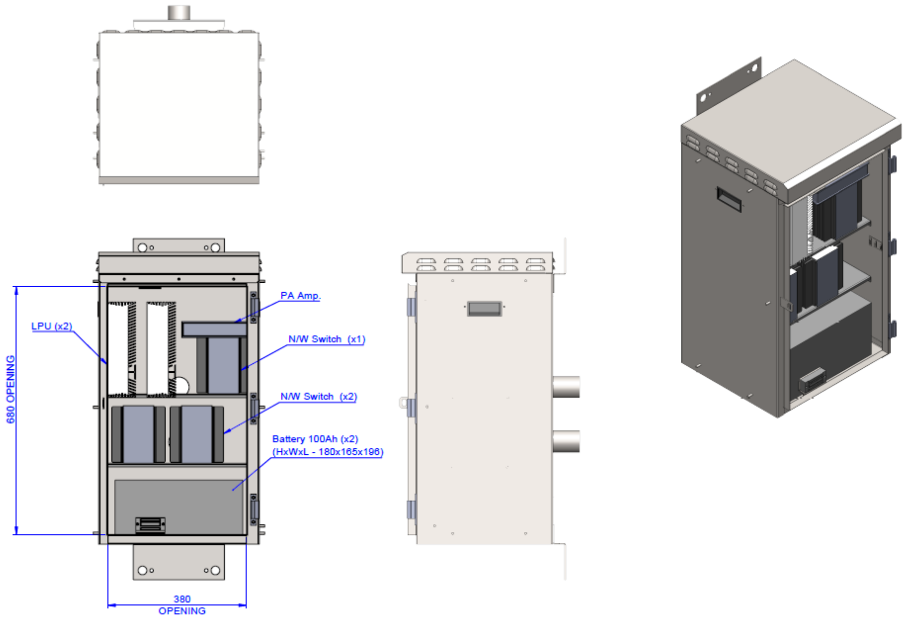
NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55

"PART B" DETAIL VIEW
DOOR CLOSD



NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55

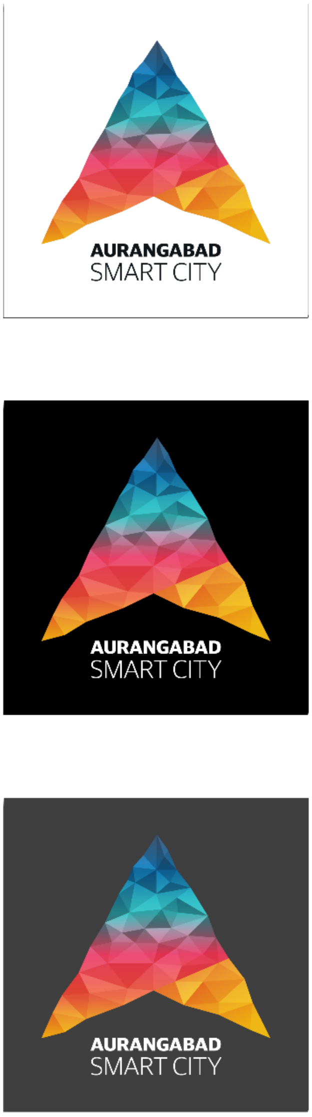
"PART B" DETAIL VIEW
DOOR OPEN

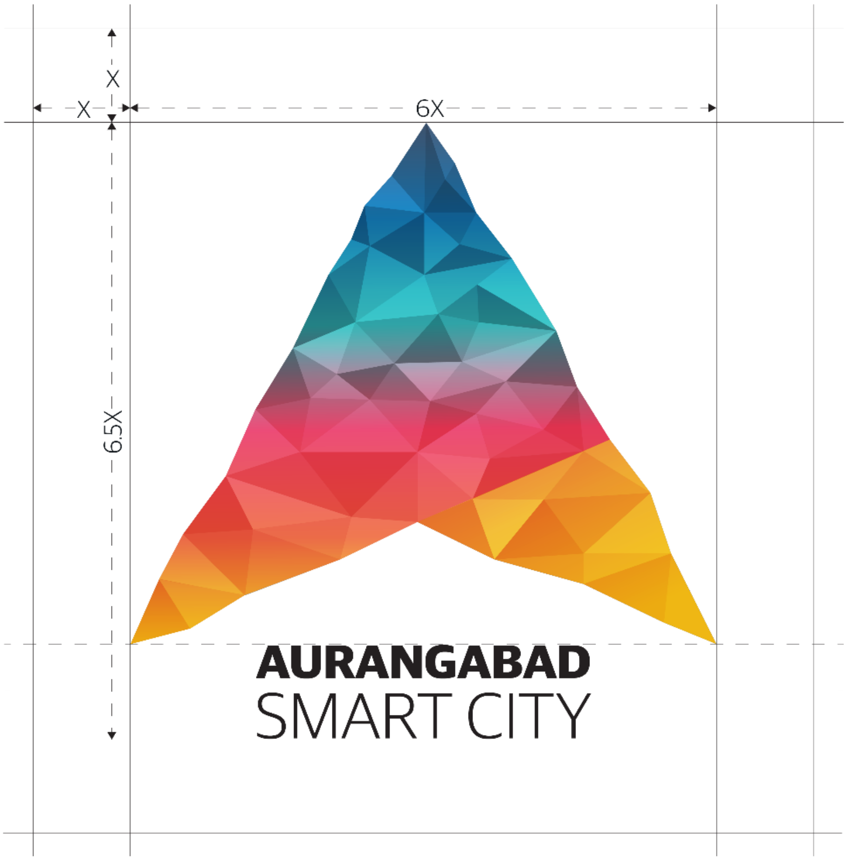


NOTE:
1. Surface Protection :- Powder Coated Delta Std.
2. Component Placement might change as per Actual.
3. IP Protection :- IP 55

12.3 Branding Guidelines

Primary Approved Identity / Background Colour Placements





Signature Colour Control

Correct use of colour is vital when reproducing the ASC identity. Care must be taken to ensure that the identity reproduces clearly on any of the approved colour backgrounds stated below.

Blue gray	Blue	Aqua green	Pink	Orange	Chrome yellow
Monitor R-55, G-71, B-92	**Monitor** R-16, G-94, B-140	**Monitor** R-42, G-145, B-145	**Monitor** R-227, G-58, B-89	**Monitor** R-225, G-81, B-54	**Monitor** R-238, G-181, B-20
Process C-82, M-67, Y-44, K-30	**Process** C-94, M-63, Y-24, K-6	**Process** C-79, M-25, Y-44, K-3	**Process** C-5, M-92, Y-56, K-0	**Process** C-6, M-83, Y-87, K-1	**Process** C-7, M-29, Y-100, K-0
Websafe #37475C	**Websafe** #105E8C	**Websafe** #2A9191	**Websafe** #E33A59	**Websafe** #E15136	**Websafe** #EEB514

Incorrect Identity Usage

The examples demonstrated on the page opposite include some exagerated possible mistakes - no coloured backgrounds for the identity with stationery, no photographic backgrounds ever, no
changes in the colours of the identity itself and no interference with the identity by type, other graphic elements and so on.

Dont's

AURANGABAD
SMART CITY

Never alter the position of any elements within the identity

AURANGABAD
SMART CITY

Never attempt to adjust or re-type any of the wordmark typography

AURANGABAD
SMART CITY

Never change the colour of the wordmark

AURANGABAD
SMART CITY

Never restrict the identity by applying a holding box or shape

AURANGABAD
SMART CITY

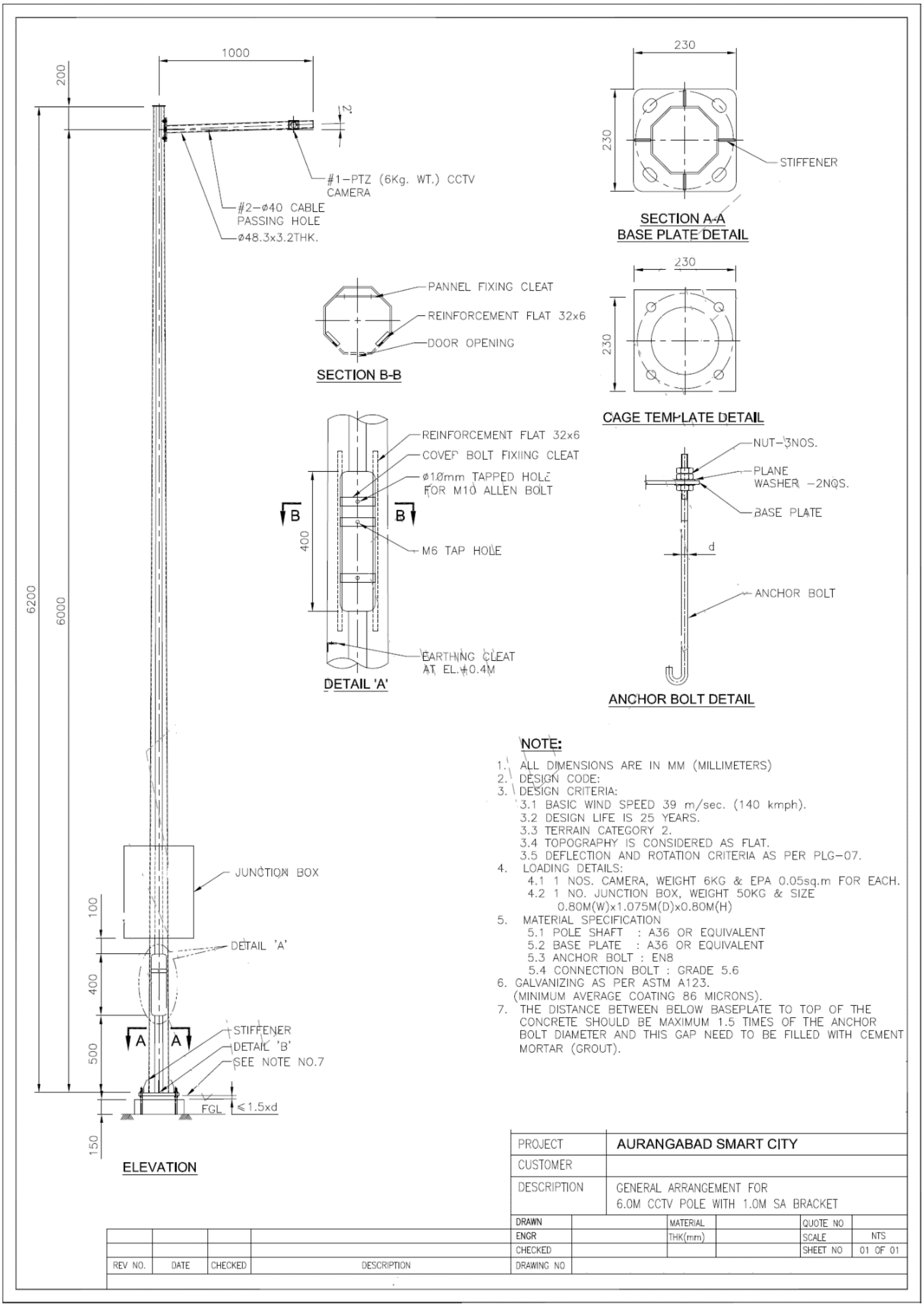
Never apply the identity to a background image. This vastly reduces legibility and recognition

AURANGABAD
SMART CITY

Never apply a background colour to the identity unless specifi ed within this guidelines document

12.4 Utility Pole for surveillance, smart traffic and Digital signage

- **6M CCTV Pole with 1M SA Brackets**



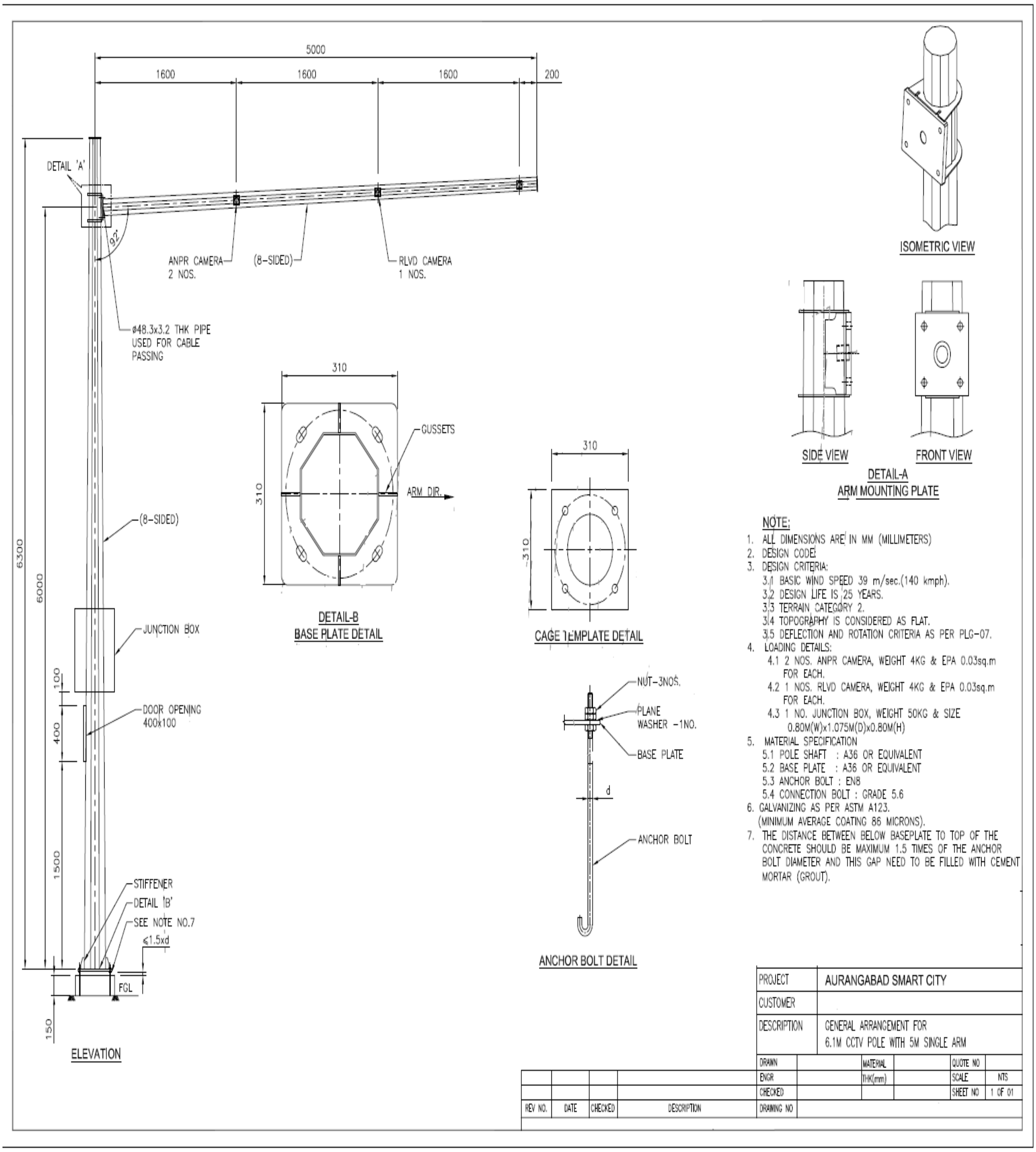
NOTE:

1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE:
3. DESIGN CRITERIA:
   3.1 BASIC WIND SPEED 39 m/sec. (140 kmph).
   3.2 DESIGN LIFE IS 25 YEARS.
   3.3 TERRAIN CATEGORY 2.
   3.4 TOPOGRAPHY IS CONSIDERED AS FLAT.
   3.5 DEFLECTION AND ROTATION CRITERIA AS PER PLG–07.
4. LOADING DETAILS:
   4.1 1 NOS. CAMERA, WEIGHT 6KG & EPA 0.05sq.m FOR EACH.
   4.2 1 NO. JUNCTION BOX, WEIGHT 50KG & SIZE 0.80M(W)x1.075M(D)x0.80M(H)
5. MATERIAL SPECIFICATION
   5.1 POLE SHAFT : A36 OR EQUIVALENT
   5.2 BASE PLATE : A36 OR EQUIVALENT
   5.3 ANCHOR BOLT : EN8
   5.4 CONNECTION BOLT : GRADE 5.6
6. GALVANIZING AS PER ASTM A123.
   (MINIMUM AVERAGE COATING 86 MICRONS).
7. THE DISTANCE BETWEEN BELOW BASEPLATE TO TOP OF THE CONCRETE SHOULD BE MAXIMUM 1.5 TIMES OF THE ANCHOR BOLT DIAMETER AND THIS GAP NEED TO BE FILLED WITH CEMENT MORTAR (GROUT).

PROJECT	AURANGABAD SMART CITY
CUSTOMER	
DESCRIPTION	GENERAL ARRANGEMENT FOR 6.0M CCTV POLE WITH 1.0M SA BRACKET

				DRAWN		MATERIAL		QUOTE NO	
				ENGR		THK(mm)		SCALE	NTS
				CHECKED				SHEET NO	01 OF 01
REV NO.	DATE	CHECKED	DESCRIPTION	DRAWING NO					

- **6.1 M CCTV Pole with 5 M single arm.**



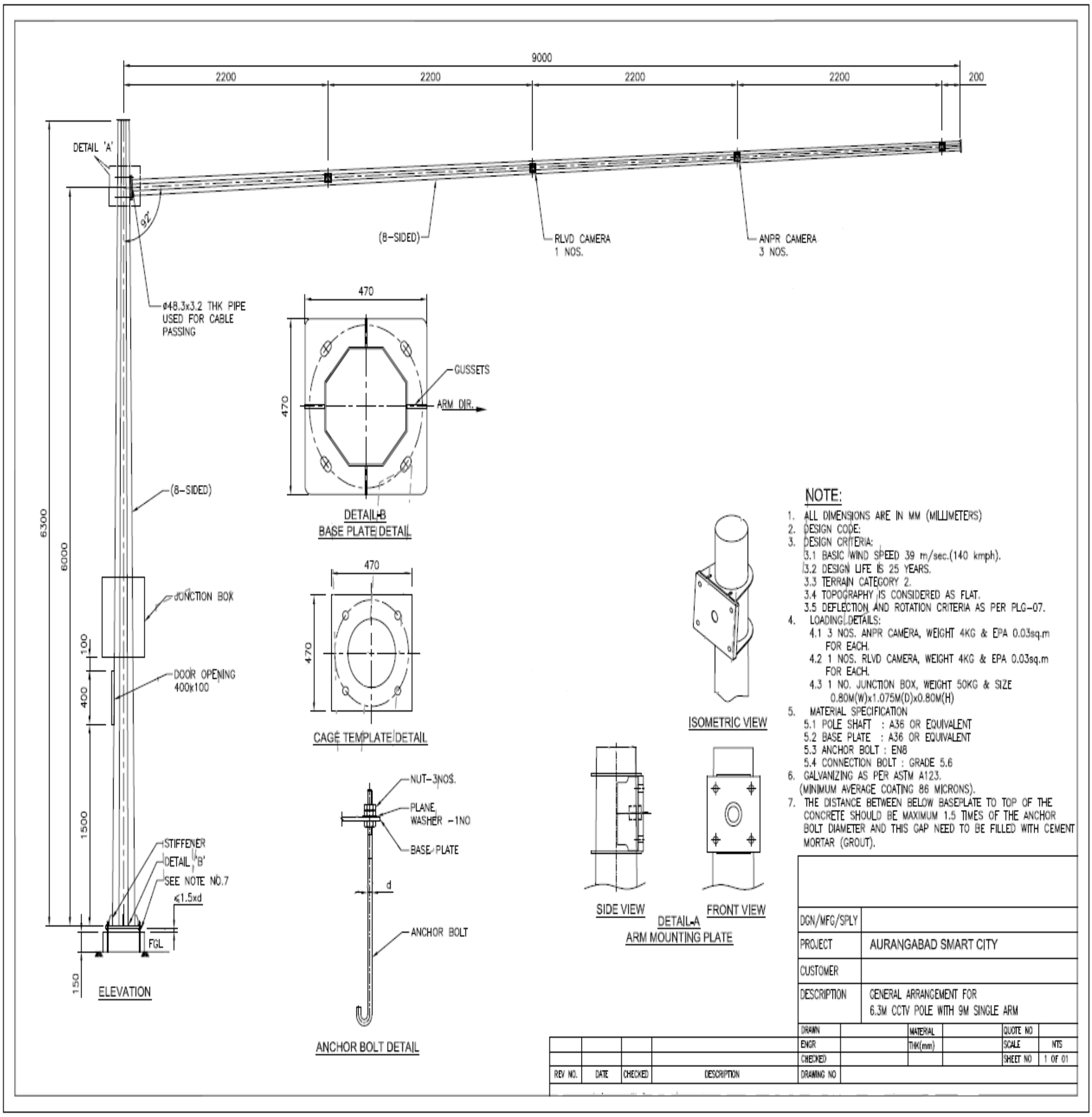
NOTE:

1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE:
3. DESIGN CRITERIA:
   3.1 BASIC WIND SPEED 39 m/sec.(140 kmph).
   3.2 DESIGN LIFE IS 25 YEARS.
   3.3 TERRAIN CATEGORY 2.
   3.4 TOPOGRAPHY IS CONSIDERED AS FLAT.
   3.5 DEFLECTION AND ROTATION CRITERIA AS PER PLG–07.
4. LOADING DETAILS:
   4.1 2 NOS. ANPR CAMERA, WEIGHT 4KG & EPA 0.03sq.m FOR EACH.
   4.2 1 NOS. RLVD CAMERA, WEIGHT 4KG & EPA 0.03sq.m FOR EACH.
   4.3 1 NO. JUNCTION BOX, WEIGHT 50KG & SIZE 0.80M(W)x1.075M(D)x0.80M(H)
5. MATERIAL SPECIFICATION
   5.1 POLE SHAFT : A36 OR EQUIVALENT
   5.2 BASE PLATE : A36 OR EQUIVALENT
   5.3 ANCHOR BOLT : EN8
   5.4 CONNECTION BOLT : GRADE 5.6
6. GALVANIZING AS PER ASTM A123. (MINIMUM AVERAGE COATING 86 MICRONS).
7. THE DISTANCE BETWEEN BELOW BASEPLATE TO TOP OF THE CONCRETE SHOULD BE MAXIMUM 1.5 TIMES OF THE ANCHOR BOLT DIAMETER AND THIS GAP NEED TO BE FILLED WITH CEMENT MORTAR (GROUT).

PROJECT	AURANGABAD SMART CITY
CUSTOMER	
DESCRIPTION	GENERAL ARRANGEMENT FOR 6.1M CCTV POLE WITH 5M SINGLE ARM

				DRAWN		MATERIAL		QUOTE NO	
				ENGR		THK(mm)		SCALE	NTS
				CHECKED				SHEET NO	1 OF 01
REV NO.	DATE	CHECKED	DESCRIPTION	DRAWING NO					

- **6.3 M CCTV Pole with 9 M single arm.**



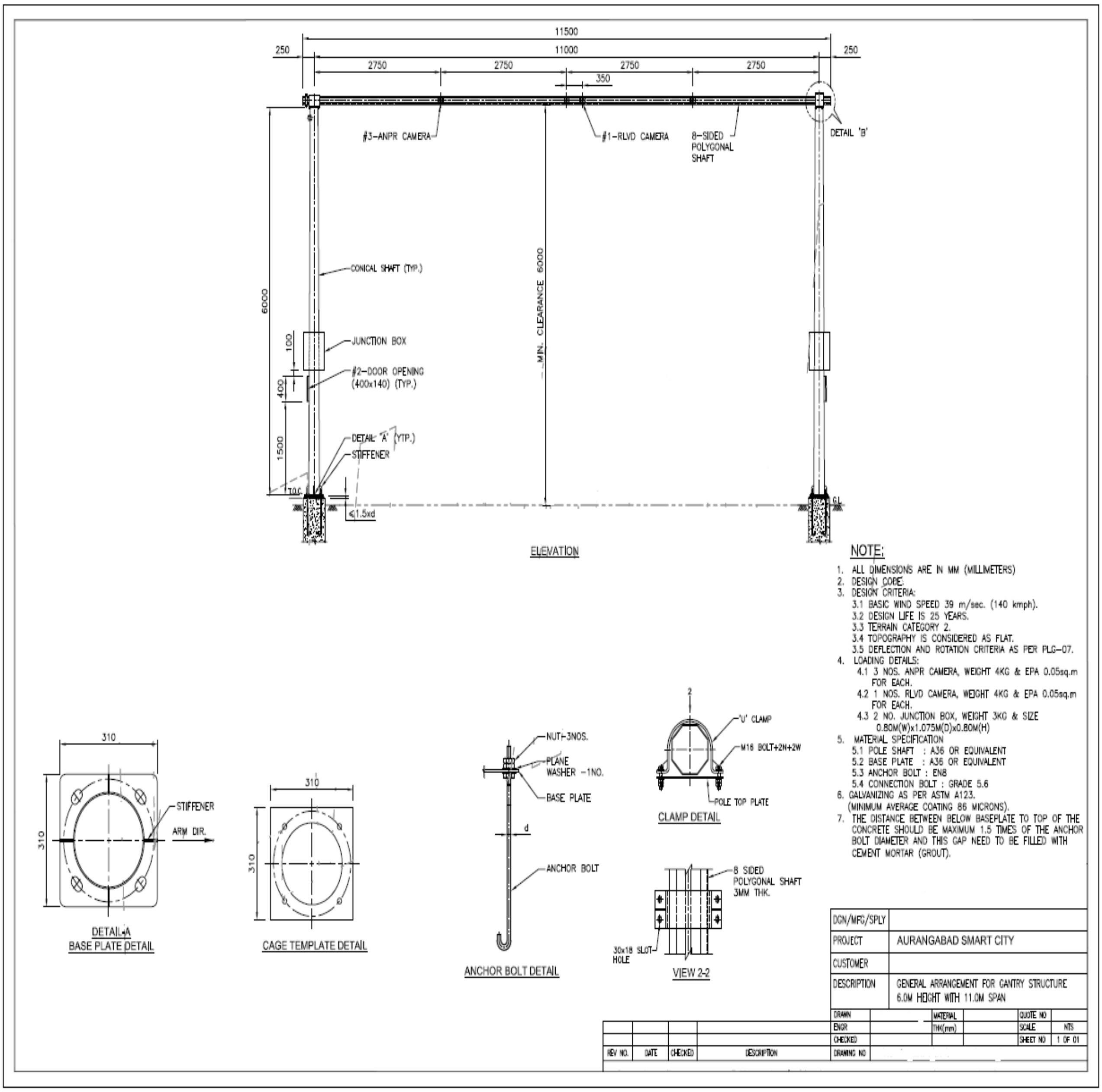
NOTE:

1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE:
3. DESIGN CRITERIA:
   3.1 BASIC WIND SPEED 39 m/sec.(140 kmph).
   3.2 DESIGN LIFE IS 25 YEARS.
   3.3 TERRAIN CATEGORY 2.
   3.4 TOPOGRAPHY IS CONSIDERED AS FLAT.
   3.5 DEFLECTION AND ROTATION CRITERIA AS PER PLG–07.
4. LOADING DETAILS:
   4.1 3 NOS. ANPR CAMERA, WEIGHT 4KG & EPA 0.03sq.m FOR EACH.
   4.2 1 NOS. RLVD CAMERA, WEIGHT 4KG & EPA 0.03sq.m FOR EACH.
   4.3 1 NO. JUNCTION BOX, WEIGHT 50KG & SIZE 0.80M(W)x1.075M(D)x0.80M(H)
5. MATERIAL SPECIFICATION
   5.1 POLE SHAFT : A36 OR EQUIVALENT
   5.2 BASE PLATE : A36 OR EQUIVALENT
   5.3 ANCHOR BOLT : EN8
   5.4 CONNECTION BOLT : GRADE 5.6
6. GALVANIZING AS PER ASTM A123.
   (MINIMUM AVERAGE COATING 86 MICRONS).
7. THE DISTANCE BETWEEN BELOW BASEPLATE TO TOP OF THE CONCRETE SHOULD BE MAXIMUM 1.5 TIMES OF THE ANCHOR BOLT DIAMETER AND THIS GAP NEED TO BE FILLED WITH CEMENT MORTAR (GROUT).

DGN/MFG/SPLY	
PROJECT	AURANGABAD SMART CITY
CUSTOMER	
DESCRIPTION	GENERAL ARRANGEMENT FOR 6.3M CCTV POLE WITH 9M SINGLE ARM

				DRAWN		MATERIAL		QUOTE NO	
				ENGR		THK(mm)		SCALE	NTS
				CHECKED				SHEET NO	1 OF 01
REV NO.	DATE	CHECKED	DESCRIPTION	DRAWING NO					

- **Gantry Structure 6 M height with 11 M span**



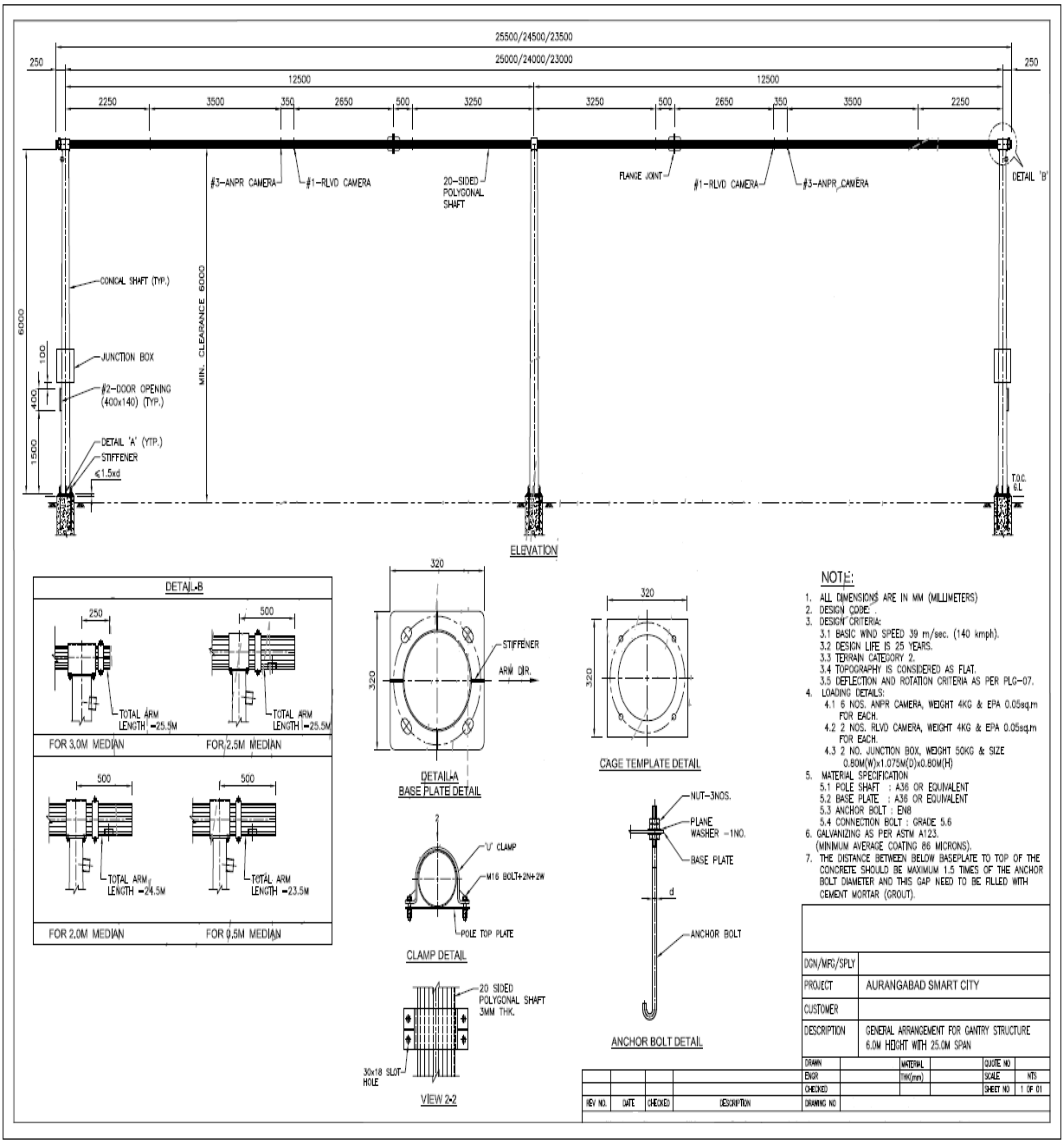
NOTE:

1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE:
3. DESIGN CRITERIA:
   3.1 BASIC WIND SPEED 39 m/sec. (140 kmph).
   3.2 DESIGN LIFE IS 25 YEARS.
   3.3 TERRAIN CATEGORY 2.
   3.4 TOPOGRAPHY IS CONSIDERED AS FLAT.
   3.5 DEFLECTION AND ROTATION CRITERIA AS PER PLG–07.
4. LOADING DETAILS:
   4.1 3 NOS. ANPR CAMERA, WEIGHT 4KG & EPA 0.05sq.m FOR EACH.
   4.2 1 NOS. RLVD CAMERA, WEIGHT 4KG & EPA 0.05sq.m FOR EACH.
   4.3 2 NO. JUNCTION BOX, WEIGHT 3KG & SIZE 0.80M(W)x1.075M(D)x0.80M(H)
5. MATERIAL SPECIFICATION
   5.1 POLE SHAFT : A36 OR EQUIVALENT
   5.2 BASE PLATE : A36 OR EQUIVALENT
   5.3 ANCHOR BOLT : EN8
   5.4 CONNECTION BOLT : GRADE 5.6
6. GALVANIZING AS PER ASTM A123. (MINIMUM AVERAGE COATING 86 MICRONS).
7. THE DISTANCE BETWEEN BELOW BASEPLATE TO TOP OF THE CONCRETE SHOULD BE MAXIMUM 1.5 TIMES OF THE ANCHOR BOLT DIAMETER AND THIS GAP NEED TO BE FILLED WITH CEMENT MORTAR (GROUT).

DGN/MFG/SPLY	
PROJECT	AURANGABAD SMART CITY
CUSTOMER	
DESCRIPTION	GENERAL ARRANGEMENT FOR GANTRY STRUCTURE 6.0M HEIGHT WITH 11.0M SPAN

				DRAWN	MATERIAL		QUOTE NO	
				ENGR	THK(mm)		SCALE	NTS
				CHECKED			SHEET NO	1 OF 01
REV NO.	DATE	CHECKED	DESCRIPTION	DRAWING NO				

- **Gantry Structure 6 M height with 25 M span**



NOTE:

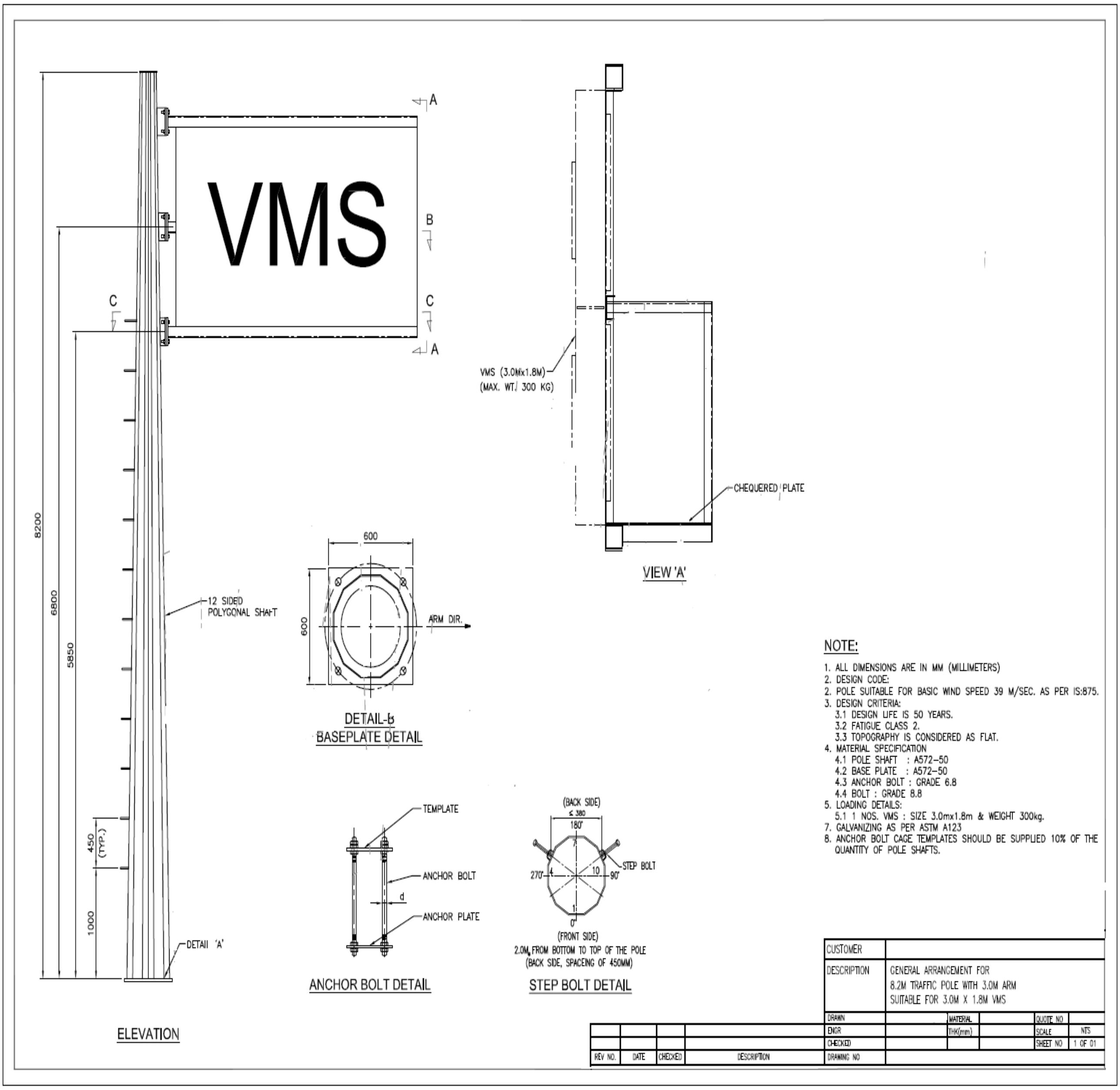
1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE: .
3. DESIGN CRITERIA:
   3.1 BASIC WIND SPEED 39 m/sec. (140 kmph).
   3.2 DESIGN LIFE IS 25 YEARS.
   3.3 TERRAIN CATEGORY 2.
   3.4 TOPOGRAPHY IS CONSIDERED AS FLAT.
   3.5 DEFLECTION AND ROTATION CRITERIA AS PER PLG–07.
4. LOADING DETAILS:
   4.1 6 NOS. ANPR CAMERA, WEIGHT 4KG & EPA 0.05sq.m FOR EACH.
   4.2 2 NOS. RLVD CAMERA, WEIGHT 4KG & EPA 0.05sq.m FOR EACH.
   4.3 2 NO. JUNCTION BOX, WEIGHT 50KG & SIZE 0.80M(W)x1.075M(D)x0.80M(H)
5. MATERIAL SPECIFICATION
   5.1 POLE SHAFT : A36 OR EQUIVALENT
   5.2 BASE PLATE : A36 OR EQUIVALENT
   5.3 ANCHOR BOLT : EN8
   5.4 CONNECTION BOLT : GRADE 5.6
6. GALVANIZING AS PER ASTM A123. (MINIMUM AVERAGE COATING 86 MICRONS).
7. THE DISTANCE BETWEEN BELOW BASEPLATE TO TOP OF THE CONCRETE SHOULD BE MAXIMUM 1.5 TIMES OF THE ANCHOR BOLT DIAMETER AND THIS GAP NEED TO BE FILLED WITH CEMENT MORTAR (GROUT).

DGN/MFG/SPLY	
PROJECT	AURANGABAD SMART CITY
CUSTOMER	
DESCRIPTION	GENERAL ARRANGEMENT FOR GANTRY STRUCTURE 6.0M HEIGHT WITH 25.0M SPAN

DRAWN		MATERIAL		QUOTE NO	
ENGR		THK(mm)		SCALE	NTS
CHECKED				SHEET NO	1 OF 01
DRAWING NO					

REV NO.	DATE	CHECKED	DESCRIPTION

- **8.2 M Traffic Pole with 3 M Arm.**

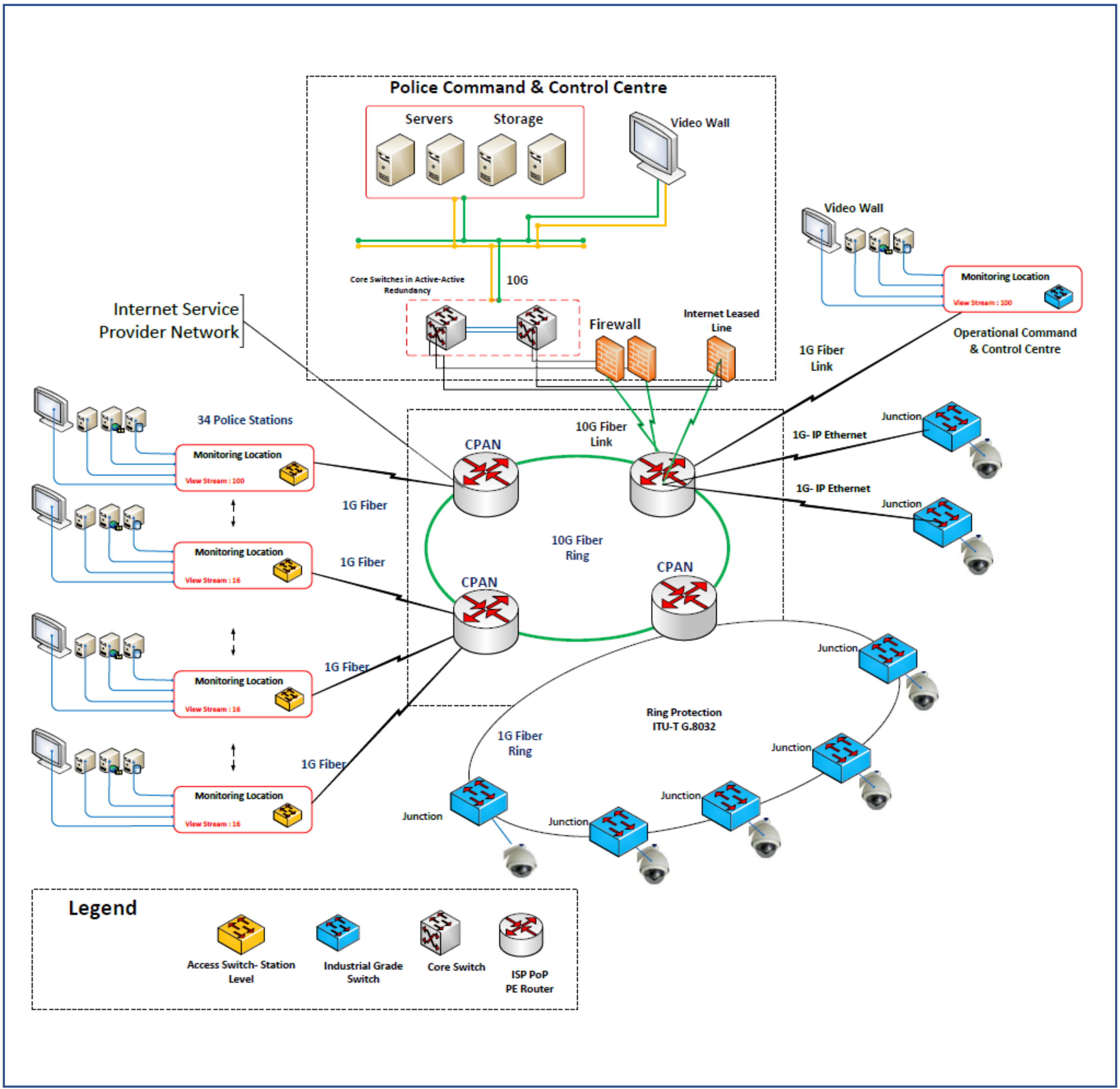


NOTE:

1. ALL DIMENSIONS ARE IN MM (MILLIMETERS)
2. DESIGN CODE:
2. POLE SUITABLE FOR BASIC WIND SPEED 39 M/SEC. AS PER IS:875.
3. DESIGN CRITERIA:
   3.1 DESIGN LIFE IS 50 YEARS.
   3.2 FATIGUE CLASS 2.
   3.3 TOPOGRAPHY IS CONSIDERED AS FLAT.
4. MATERIAL SPECIFICATION
   4.1 POLE SHAFT : A572-50
   4.2 BASE PLATE : A572-50
   4.3 ANCHOR BOLT : GRADE 6.8
   4.4 BOLT : GRADE 8.8
5. LOADING DETAILS:
   5.1 1 NOS. VMS : SIZE 3.0mx1.8m & WEIGHT 300kg.
7. GALVANIZING AS PER ASTM A123
8. ANCHOR BOLT CAGE TEMPLATES SHOULD BE SUPPLIED 10% OF THE QUANTITY OF POLE SHAFTS.

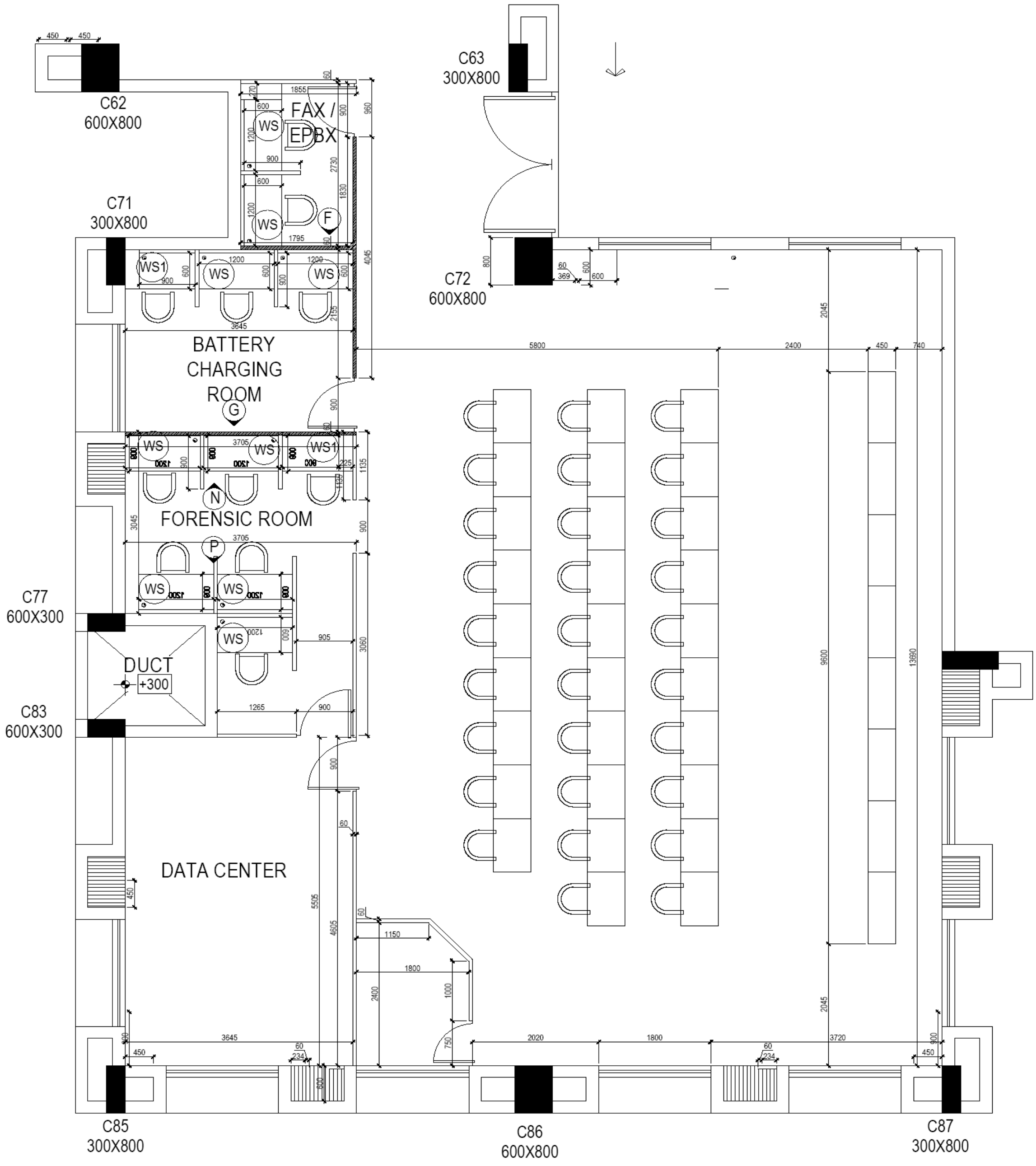
				CUSTOMER					
				DESCRIPTION	GENERAL ARRANGEMENT FOR 8.2M TRAFFIC POLE WITH 3.0M ARM SUITABLE FOR 3.0M X 1.8M VMS				
				DRAWN		MATERIAL		QUOTE NO	
				ENGR		THK(mm)		SCALE	NTS
				CHECKED				SHEET NO	1 OF 01
REV NO.	DATE	CHECKED	DESCRIPTION	DRAWING NO					

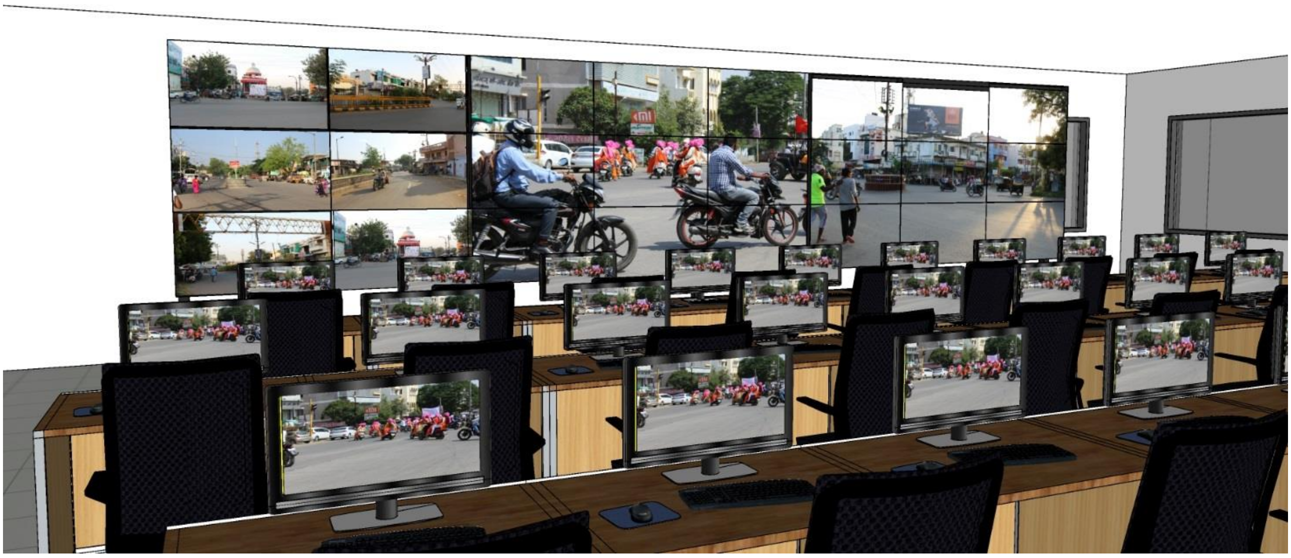
12.5 City Network



12.6 Control and command centre

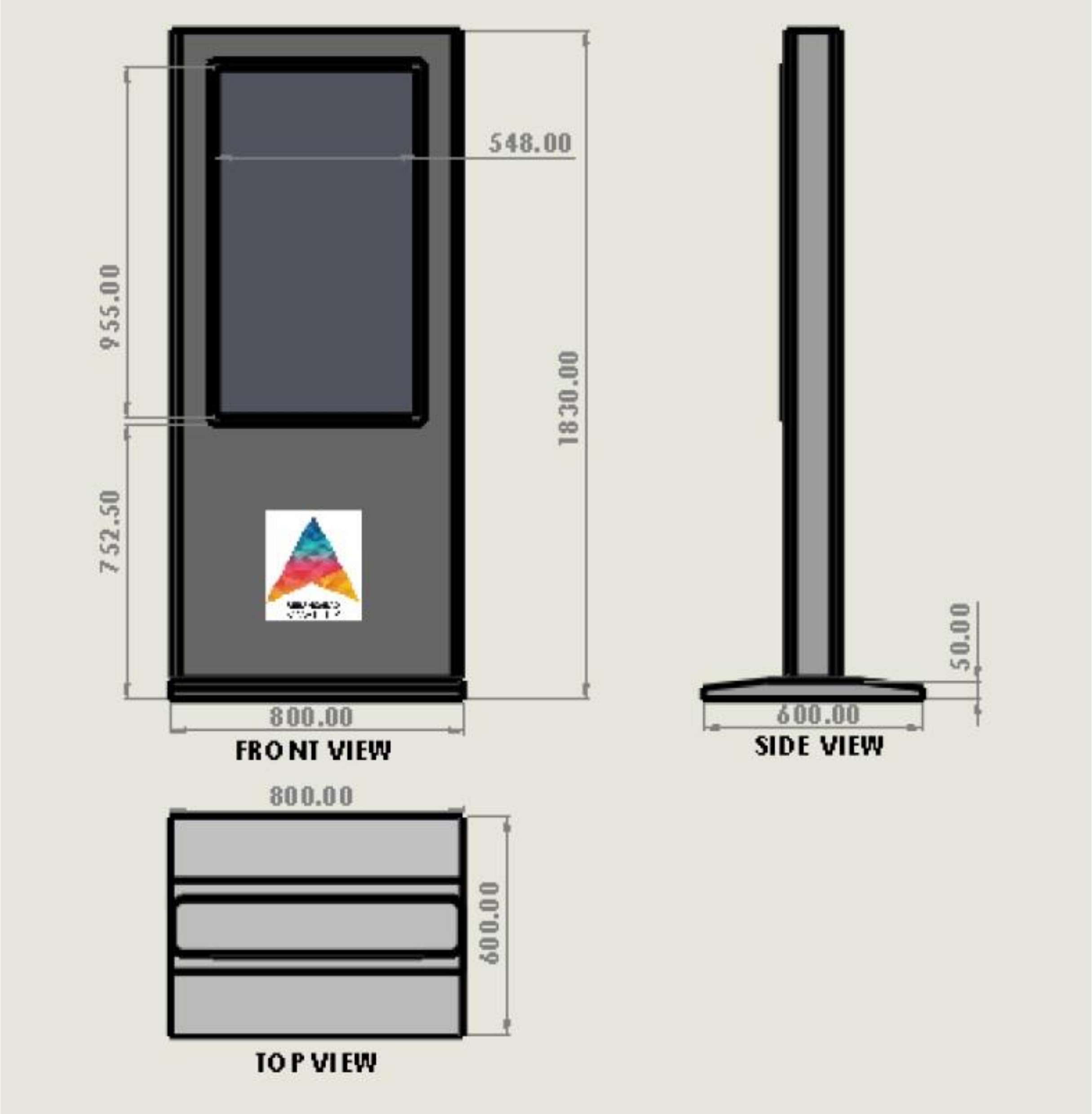
Layout Plan for Control and Command Centre of Police





12.7 Kiosk

WELCOME
AURANGABAD
SMART CITY


548.00
955.00
1830.00
752.50
800.00
FRONT VIEW
50.00
600.00
SIDE VIEW
800.00
600.00
TOP VIEW

Annexure 13: Indicative length of City Network Backbone

Details on City Network Back bone

Sl. #	Area within the city*	Length of the network to be laid
		Total (KM)

* Enclose a map showing area and alignment of network to be laid

Annexure 14: Information on City Bus Services

A. Category wise fleet size

Sl. #	Fleet Size	

B. Number and Location of Bus stops (along with Map)

Sl. #	Bus Stops Locations

C. Location of Bus depots (along with Map)

Sl. #	Bus Stops Locations

Annexure 15: ICT based Solid Waste Management System

A. Location of Secondary collection points

Sl. #	Locations of secondary collection points

B. Location of Bins (to be RFID tagged)

Sl. #	Locations of secondary collection points

C. Category wise fleet size for Solid Waste Collection and Transportation

Fleet Size	
Type of vehicle	Number

Annexure 16: Manufacturer's Authorization (To be obtained from all OEMs)

To,

WHEREAS who are official manufacturers --of having factories at---do here by authorize----------------------------------to submit a Bid in relation to the Invitation for Bids indicated above, the purpose of which is to provide the following Goods, manufactured by us--------------------------------and to subsequently negotiate and sign the Contract.

We hereby extend our full guarantee and warranty in accordance with the requirement mentioned in tender documents with respect to the Goods offered by the above firm in reply to this Invitation for Bids.

Name:

In the capacity of:

Signed:

Duly authorized to sign the Authorization for and on behalf of Date:

[Signature] - [Company Seal]

Annexure 17: Equipment Details

Sr. No.	Item Description	Specification	Manufacturing Company	Make and Model

Details should be submitted for each equipment mentioned in BoM with technical details along with Datasheets.

Name:
In the capacity of:
Signed:
Duly authorized to sign the Authorization for and on behalf of Date:
[Signature] - [Company Seal]

Annexure 18: Deviation

We hereby declare that there is no deviation in our proposal from your RFP. OR

List of Deviations

Sr. No.	RFP Page No.	Requirement As per RFP	Deviation As Per our Proposal

Name:

In the capacity of:

Signed:

Duly authorized to sign the Authorization for and on behalf of Date:

[Signature] - [Company Seal]

Annexure 19: Organization Detail

Name of Organization	
Registration Date	
Details of Primary Contact Person	
Name	
Designation	
Office Address	
Telephone and Fax No.	
E-mail	
Registration Type	**Number**
Permanent Account Number	
MP VAT TIN Registration No.	
CST Registration No.	
Service Tax Registration No.	

Name:

In the capacity of:

Signed:

Duly authorized to sign the Authorization for and on behalf of

Date: [Signature] - [Company Seal]

Annexure 21: Project Implementation Methodology and Scalability

The Bidder is required to submit the proposed technical solution in detail. Following should be captured in the explanation:

a. The Overall approach to the Project.

b. Implementation Methodology and Strategy.

c. Project Organization and Management Plan.

d. Project Monitoring and Communication Plan– Bidder’s approach to project monitoring and communications among stakeholders.

e. Implementation plan– Bidder’s approach to implement the project.

f. Risk Management Plan – Bidder’s approach to identify, respond / manage and mitigate risks.

g. Quality Control plan - Bidder's approach to ensure quality of work and deliverables.

h. Escalation matrix during contract period.

Note:

1. All the pages (documentary proofs and other documents that may be attached) should contain page numbers and would have to be uniquely serially numbered.

2. Inadequate information shall lead to disqualification of the bid.

Annexure 22: Undertaking of Providing Training

Date:

To,

Sir,

In response to the tender Reference No: I as an owner/Partner/Director of <<Name of Bidder>>, I/We hereby declare that I/We/Our Company <<Name of Bidder>>

Will train manpower and provide proper hand holding support to client as and when needed by client/Tenderer during and after the tenure of project, and I/We will furnish help manual for the entire system with FAQ and general troubleshooting guide.

Name:

In the capacity of:

Signed:

Duly authorized to sign the Authorization for and on behalf of Date:

[Signature] [Company Seal]

Annexure 23: Undertaking Of Blacklisting

Date:

To,

Sir,

In response to the tender Reference No: I as an owner/Partner/Director of <<Name of Bidder>>, I/We hereby declare that <<Name of Bidder>>, is having unblemished past record and was not declared ineligible for corrupt and fraudulent practices and/or blacklisted either indefinitely or for a particular period of time by any State government/ Central Government / semi government / PSU / Municipal agencies in India.

Name:

In the capacity of:

Signed:

Duly authorized to sign the Authorization for and on behalf of Date:

[Signature] - [Company Seal]

Annexure 24: Standards and Guidelines

24.1 Annex-A (Biometric Standard)

Biometric Standards

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: ○ Characteristics of Face Image capturing device ○ Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification

	○ Scene requirements of the face images, keeping in view a future possibility of computer based face recognition ○ Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

2) Fingerprint Image and Minutiae Data Standard

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching.

It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1 (verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification / identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

Standard	Description
ISO/IEC 19794-4:2005(E)	This standard deals with usage of fingerprint image data and minutiae data for identification and verification of an individual. To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1. The Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard

	specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements. The current version of the standard is applicable to all civilian e-governance applications as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

3) Iris Image Data Standard

In the recent years, Iris recognition has emerged as an important and powerful Biometric characteristic. The Indian Government anticipates that, iris biometric would be deployed for identification and verification in e-Governance applications where identity management is a major issue.

In order to capture the Iris image, special devices are available in the market providing different formats for image acquisition and storage. Also many algorithms have been developed by vendors to extract the features of iris images to decide on a match during verification / identification stage. To ensure interoperability among the e-Governance applications requiring iris recognition, it is necessary to standardize iris specifications including the storage and transmission formats.

Thus, to allow the application developer maximum flexibility in usage of algorithms and devices from different vendors and to address interoperability requirements, the iris image must be captured and stored as per standard specifications included in this document.

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

There are two types of interchange formats to represent the Iris image data. The first is a rectilinear (rectangular or Cartesian) image storage format that specifies raw, uncompressed or compressed intensity values. The second format is based on polar image specification with specific pre processing and segmentation steps, producing a compact data structure containing only Iris information.

The Indian e-Governance applications will deal with Iris image data during multiple stages. Some of these stages are given below:

a. Image acquisition, its processing and its storage in the Enrolment stage
b. Image acquisition and storage for off line / on line verification of Iris image data in 1:1 matching stage
c. Image acquisition and storage for the purpose of identification in 1:N matching stage
d. Transmission of Iris image data to other e-Governance applications
e. Extraction of features of Iris images (enrolment or recognition stage), their storage, and matching (Not covered in the present version of the standard).

The interchange format type of the Iris images that is defined in this standard is for **rectilinear images only**.

If the image is collected by a camera that captures only one eye at a time and is stored using a rectilinear coordinate system no specific pre-processing is required. Cameras that capture images of both eyes simultaneously may use the following processing steps to calculate the rotation angle of the Iris images.

Standard	Description
ISO/IEC 19794-4:2005(E)	The Government of India would broadly adopt ISO 19794-6:2005(E) Iris Image Data Standard, by tailoring the standard specifications to meet specific needs of civilian e-Governance applications in Indian context and as per the GoI Policy on Open Standards. This Standard specifies Iris image data specifications, acquisition, storage and transmission formats. It also includes best practices for implementation of the Standard specifications in different categories of e-Governance applications, based on the volume of data and verification/ accuracy requirements. This version of the Standard does not include features extraction & matching specifications.

Reference Standards:

1. GoI Face Image data standard version 1.0 published in November, 2010
2. GoI Fingerprint Image data Standard version 1.0 published in November, 2010
3. GoI Iris Image Data Standard Version 0.4, document published in March, 2011

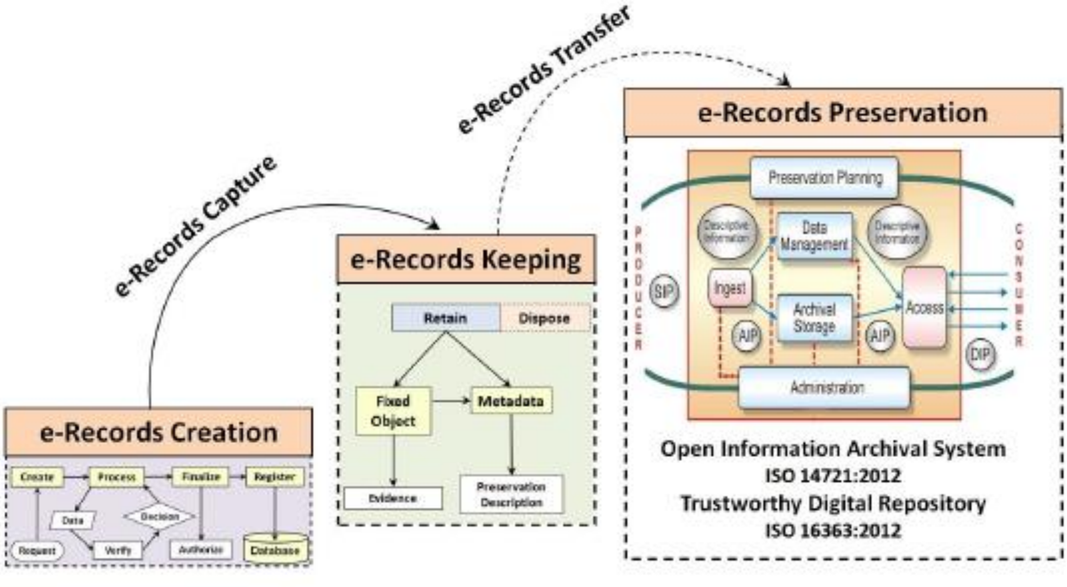
24.2 Annex-B (Digital Preservation Standards)

The **e-Governance Standard for Preservation Information Documentation (eGOV-PID) of Electronic Records (eGOV-PID)** provides a standardized metadata dictionary and schema for describing the "preservation metadata" of an electronic record. This standard proposes to capture most of the preservation information (metadata) automatically after the final e-record is created by the e-Government system. Such preservation information documentation is necessary only for those e-records that need to be retained for long durations (e.g. 10 years, 25 years, 50 years and beyond) and the e-records that need to be preserved permanently.

The implementation of this standard helps in producing the valid input i.e. Submission Information Package (SIP) for archival and preservation purpose as per the requirements specified in the ISO 14721 Open Archival Information Systems (OAIS) Reference Model.

The eGOV-PID allows to capture the preservation metadata in terms of cataloguing information, enclosure information, provenance information, fixity information, representation information, digital signature information and access rights information.

The core concepts of 'preservability' are based on the requirements specified in IT ACT, ISO/TR 15489-1 and 2 Information Documentation - Records Management and ISO 14721 Open Archival Information Systems (OAIS) Reference Model. It introduces 5 distinct steps of e-record management i.e. e-record creation, e-record capturing, e-record keeping, e-record transfer to designated trusted digital repository and e-record preservation which need to be adopted in all e-Governance projects.



Standard	Description
ISO 15836:2009	Information and documentation - The Dublin Core metadata elements
ISO/TR 15489-1 and 2	Information and Documentation - Records Management: 2001
ISO 14721:2012	Open Archival Information Systems (OAIS) Reference Model
ISO/DIS 16363: 2012	Audit & Certification of Trustworthy Digital Repositories
METS, Library of Congress, 2010	Metadata Encoding and Transmission Standard (METS) -
InterPARES 2	International Research on Permanent Authentic Records - A Framework of Principles for the Development of Policies, Strategies and Standards for the Long-term Preservation of Digital Records, 2008
ISO 19005-1:2005 Use of PDF 1.4 (PDF/A-1b) with Level B	Capture of e-records in PDF for Archival (PDFA) format - PDF/A-1a is based on the PDF Reference Version 1.4 from Adobe Systems Inc. (implemented in Adobe Acrobat 5 and latest versions) and is defined by ISO 19005-1:2005. Conformance is recommended for archival of reformatted digital documents due to following reasons: o PDF/A-1b preserves the visual appearance of the document o Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** o Apache FOP 1.1 library can be used in the application logic for dynamically publishing the e-records in PDF/A format. **PDF/A for document creation** o Libre Office 4.0 supports the exporting of a document in PDF/A format. o MS Office 2007 onwards the support for “save as” PDF/A is available. o Adobe Acrobat Professional can be used for converting the PDF documents to PDF/A format.
ISO 19005-2:2011 Use of ISO 32000-1 (PDF/A-2)	Recommended for preservation of documents requiring the advanced features supported in it. PDF/A-2a is based on ISO 32000-1 – PDF 1.7 and is defined by ISO 19005-2:2011. Its features are as under: o Support for JPEG2000 image compression o Support for transparency effects and layers o Embedding of OpenType fonts o Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard o Possibility to embed PDF/A files in PDF/A-2 for archiving of sets of documents as individual documents in a single file PDF/A-2 does not replace the PDF/A-1 standard but it co-exists alongside with an extended set of features.

	PDF/A-1a and PDF/A-1b compliance are minimum essential for e-government records as recommended in the IFEG technical standard of DeitY.
JPEG2000 (ISO/IEC 15444-1:2004) and PNG (ISO/IEC 15948:2004)	Image file formats - which support lossless compression are recommended as raster image file formats for e-governance applications as specified in Technical Standards for Interoperability Framework for e-Governance (IFEG) in India, published in 2012 by e-Gov Standards Division, DeitY.
ISO/IEC 27002: 2005	Code of practices for information security management for ensuring the security of the e-records archived on digital storage.

24.3 Annex-C (Localization and Language Technology Standard)

1. Character Encoding Standard for Indian Languages

The lack of availability of information in the locally understandable language is the main reason for the slow progress in the Information and Communication Technology (ICT) sector. In today's age, access to ICT plays a major role in the overall development of a country, it has become a challenge to bridge the digital divide caused by the language barrier.

Standardisation is one of the baselines to be followed in localisation. Standardisation means to follow certain universally accepted standards, so that the developers from any part of the globe could interact through the application. Standardisation becomes applicable in almost everything specific to the language – for instance, a standard glossary of terms for translation, a standard keyboard layout for input system, a standard collation sequence order for sorting, a standard font etc.

Character Encoding standard for all constitutionally recognized Indian Languages should be such that it facilitates global data interchange.

ISCII is the National Standard and Unicode is the global character encoding standard.The average data packet size is less for representation of any Indian languages using ISCII. However, being limited code space, coexistence of multiple languages within the same code page is not possible in ISCII. The migration from ISCII to Unicode has become imperative due to the following reasons:

All major operating systems, browsers, editors, word processors and other applications & tools are supporting Unicode.

- It is possible to use Indian languages and scripts in the Unicode environment, which will resolve the compatibility issue.
- The documents created using Unicode may be searched very easily on the web.
- As Unicode is widely recognized all over the world and also supporting Indian languages, it will ease Localization applications including e-Governance application for all the constitutionally recognized Indian languages.
- Since Indian languages are also used in the other part of the world, it is possible to have Global data exchange.

Unicode shall be the storage-encoding standard for all constitutionally recognised Indian Languages including English and other global languages as follows:

Specification Area	Standard Name	Owner	Nature of the Standard	Nature of Recommend Actions
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode	Unicode Consortium, Inc.	Matured	Mandatory

	consortium from time to time.			

Character: Character is the smallest component of any written language that has semantic value.

ISCII: Indian Script Code for Information Interchange (ISCII - IS 13194:1991) is the character-encoding standard approved by Bureau of Indian Standards (BIS). ISCII is an 8 bit-encoding scheme, catering to 128 code spaces for representation of Indian languages.

Nine Indian scripts are included in ASCII standard to represent 10 Indian languages i.e. Assamese, Bengali, Devnagari, Gujarati, Gurmukhi, Kannada, Malayalam, Oriya, Tamil and Telugu.

Unicode: Unicode is a 16-bit character-encoding standard. All the major written scripts of the world are included in the Unicode Standard. The first version of Unicode was published in year 1991.

Unicode vis-à-vis ISO10646

Unicode is a 16 bit Character Encoding standard. All the major written scripts are included in the Unicode Standard. Indian scripts are also included in the standard. There are 22 constitutionally recognised Indian Languages, written in 12 different scripts. ISO/IEC 10646 is the character-encoding scheme evolved by the International Organisation for Standardisation (ISO) in 1990.

In 1991, the ISO Working Group responsible for ISO/IEC 10646 (JTC 1/SC 2/WG 2) and the Unicode Consortium decided to create universal standard for coding multilingual text. Since then, the ISO 10646 Working Group (SC 2/WG 2) and the Unicode Consortium are working together closely to extend the standard and to keep their respective versions synchronised.

In addition to the code tables as per ISO/IEC 10646, the Unicode Standard also provides an extensive set of character specifications, character data, algorithms and substantial technical material, which is useful for developers and implementers.

2. Font Standard for Indian Languages

A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

True Type Fonts (TTF) was used in various applications earlier by various vendors. TTF had no encoding standard due to which vendors and developers had their own encoding schemes, thereby jeopardizing data portability. ISO/IEC 14496-OFF (Open Font Format) on the other hand is based on a single International Standard and complies with UNICODE for data storage.

This ensures data portability across various applications and platforms. Open type font is a smart font which has built- in script composition logic.

Most often it has been observed that the use of proprietary fonts of different standards in Government Offices, which are not compatible with each other, is causing serious problems in information exchange amongst offices. By using Unicode compliant ISO/IEC 14496-OFF (Open Font Format) for font standard, the problem relating to the exchange of documents/files is completely solved.

Open standard under the International Organization for Standardization (ISO) within the MPEG group, which had previously adopted Open Type by reference, now adopted the new standard with appropriate language changes for ISO, and is called the "ISO/IEC 14496-OFF (Open Font Format)" for which formal approval reached in March 2007 as ISO Standard ISO/IEC 14496-OFF (Open Font Format) and it is a free, publicly available standard.

ISO/IEC 14496-OFF (Open Font Format) for font standard would be the standard for Indian Languages in e-Governance Applications. **ISO/IEC 14496-OFF (Open Font Format) for font standard is mandatory for all 22 constitutionally recognized languages.**

TTF (True Type Font)

A Font Format developed by Apple and licensed to True type, is the native Operating System Font Format for Windows and Mac operating systems.

ISO/IEC 14496-OFF (Open Font Format)

OFF fonts allow the handling of large glyph sets using Unicode encoding. Such encoding allows broad international support for typographic glyph variants.

OFF fonts may contain digital signatures, which enable operating systems and browsing applications to identify the source and integrity of font files, (including the embedded font files obtained in web documents), before using them. Also, font developers can encode embedding restrictions in OFF fonts which cannot be altered in a font signed by the developer.

24.4 Annex-D (Metadata and Data Standards)

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

Data Standards may be defined as the agreed upon terms for defining and sharing data. Data Standards promote the consistent recording of information and are fundamental to the efficient exchange of information. They provide the rules for structuring information, so that the data entered into a system can be reliably read, sorted, indexed, retrieved, communicated between systems, and shared. They help protect the long-term value of data.

Once the data standards are in place, there is a need to manage data, information, and knowledge. Metadata of standardized data elements can be used for this purpose.

Metadata is structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is often called data about data or information about information. A metadata is a matter of context or perspective -what is metadata to one person or application can be data to another person or application.

In other words, Metadata facilitates the user by providing access to the raw data through which the user can have an understanding of the actual data. Hence, Metadata is an abstraction layer that masks the underlying technologies, making the data access friendlier to the user.

Data and Metadata Standards provide a way for information resources in electronic form to communicate their existence and their nature to other electronic applications (e.g. via HTML or XML) or search tools and to permit exchange of information between applications.

The present document “Data and Metadata Standards- Demographic” focuses on Person Identification and Land Region codifications. It includes the following:

a) **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.

b) **Generic data elements** specifications like:

- Generic data elements, common across all Domain applications
- Generic data elements for Person identification
- Generic data elements for Land Region Codification
- Data elements to describe Address of a Premises, where a Person resides

c) **Specifications of Code Directories like:**

- Ownership with rights to update
- Identification of attributes of the Code directories
- Standardization of values in the Code directories

d) Metadata of Generic Data Elements

- Identification of Metadata Qualifiers
- Metadata of the data elements

e) Illustration of data elements to describe:

- Person identification
- Address of a premises

This Standard would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards (refer http://egovstandards.gov.in/policy/policy-onopen-standards-for-e-governance/)

Reference Standards:

4. ISO Standard 1000:1992 for SI Units
5. MNIC Coding for Person Identification
6. ISO 693-3 for International language codes
7. RGI's coding schemes for Languages
8. Top level document provided by Working Group on Metadata and Data Standards
9. EGIF (e- Government Interoperability Framework) Standard of U.K.
10. uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
11. http:// www.dolr.nic.in for conversion table of units as used by Department of Land Records
12. GoI Policy on open standards version 1.0 released in November, 2010
13. UID DDSVP Committee report, Version 1.0, Dec 09, 2009

14. ANSI92 Standard

24.5 Annex-E (Mobile Governance)

Framework for Mobile Governance (m-Governance)

Mobile Governance (m-Governance) is a strategy and its implementation to leverage available wireless and new media technology platforms, mobile phone devices and applications for delivery of public information and services to citizens and businesses.

The m-Governance framework of Government of India aims to utilize the massive reach of mobile phones and harness the potential of mobile applications to enable easy and round the-clock access to public services, especially in the rural areas**.** The framework aims to create unique infrastructure as well as application development ecosystem for m-Governance in the country.

In cognizance of the vast **mobile phone subscriber base, peaked to more than 1 billion usersin the country**, the Government has decided to also provision for access of public services through mobile devices, thereby establishing mobile Governance (m-Governance) as a compelling new paradigm.

Government of India will progressively adopt and deploy m-Governance in a time-bound manner to ensure inclusive delivery of public services to both the urban and rural populace in the country in accordance with this framework.

The following are the main measures laid down:

i. Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.

ii. **Open standards** shall be adopted for mobile applications for ensuring the interoperability of applications across various operating systems and devices as per the Government Policy on Open Standards for e-Governance.

iii. **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

iv. All Government Departments and Agencies shall develop and deploy mobile applications for providing all their public services through mobile devices to extent feasible on the mobile platform. They shall also specify the service levels for such services.

The success of the proposed initiative on m-Governance will greatly depend upon the ability of the Government Departments and Agencies to provide frequently needed public services to the citizens, create infrastructure for anytime anywhere mobile-based services, adopt appropriate open standards, develop suitable technology platforms, make the cost of services affordable, and create awareness, especially for people in underserved areas.

To ensure the adoption and implementation of the framework in a time-bound manner, following actions will be taken:

1. **Creation of Mobile Services Delivery Gateway (MSDG)**

   MSDG is the core infrastructure for enabling the availability of public services through mobile devices. This will be developed and maintained by an appropriate agency within DIT. MSDG is proposed to be used as a shared infrastructure by the Central and State Government Departments and Agencies at nominal costs for delivering public services through mobile devices.

   Various channels, such as voice, text (e-mail and SMS), GPRS, USSD, SIM Toolkit (STK), Cell Broadcast (CBC), and multimedia (MMS) will be incorporated to ensure that all users are able to access and use the mobile based services. The various delivery channels are expected to entail innovative ways of providing existing services as well as development of new services.

   To ensure successful implementation of the platform with requisite levels of security and redundancy, following actions will be taken:

   a) **End User Interface:** End-user devices include landline phones, mobile phones, smart phones, personal digital assistants (PDAs), tablets, and laptops with wireless infrastructure. Mobile applications developed shall take into consideration appropriately the wireless-device interface issues, such as bandwidth limitations, micro-browser and micro-screen restrictions, memory and storage capacities, usability, etc.

   b) **Content for Mobile Services:** Due to lower-bandwidth and smaller-screen characteristics of mobile devices, successful development and deployment of m-Governance will require development of separate mobile-ready content. Similarly, to meet the needs of all the potential users, the applications will need to be developed in the relevant local languages for the various channels of delivery. Open standards and open source software, to the extent possible, will be used to ensure interoperability and affordability of the content and applications developed.

   c) Mobile Applications (Apps) Store: A mobile applications (m-apps) store will be created to facilitate the process of development and deployment of suitable applications for delivery of public services through mobile devices. The m-apps store shall be integrated with the MSDG and it shall use the MSDG infrastructure for deployment of such applications. It is proposed that the store will be based upon service oriented architecture and cloud based technologies using open standards as far as practicable. The open platform will be developed and deployed in conjunction with the MSDG for making the additional value added services available to the users irrespective of the device or network operator used by them

   d) Application Programming Interfaces (APIs) for Value-Added Services (VAS) providers: MSDG shall offer suitable APIs to VAS providers with appropriate terms and conditions to ensure interoperability and compliance with standards for development of applications for delivery of public services.

e) **Mobile-Based Electronic Authentication of Users**: For electronic authentication of users for mobile-based public services, MSDG shall incorporate suitable mechanisms including Aadhaar-based authentication. This will also help in ensuring appropriate privacy and confidentiality of data and transactions.

f) **Payment Gateway**: MSDG shall also incorporate an integrated mobile payment gateway to enable users to pay for the public services electronically.

g) **Participation of Departments**: The Government Departments and Agencies both at the Central and State levels will be encouraged to offer their mobile-based public services through the MSDG to avoid duplication of infrastructure.

2. Creation of Mobile Governance Innovation Fund

Department of Information Technology (DIT) shall create a Mobile Governance Innovation Fund to support the development of suitable applications by Government Departments and Agencies and also by third-party developers including start-ups. The fund shall be created and managed by DIT for a minimum period of 3 years. The objective of this fund will be to accelerate the development and deployment of the mobile applications across the entire spectrum of public services.

3. Creation of Knowledge Portal and Knowledge Management Framework on Mobile Governance

DIT shall develop and deploy a state-of-the-art knowledge portal and knowledge management framework that acts as a platform for awareness generation and dissemination for various Central Government Ministries and the State Governments. This will enhance the absorptive as well as the service provision capabilities of various stakeholders in m-Governance. Since m-Governance is in its nascent stage both in India and globally, the knowledge portal will act as a reference and guide for Government Departments and Agencies in India.

4. Creation of Facilitating Mechanism

An appropriate facilitating mechanism will be created to ensure compliance with the standards for mobile applications and ensure seamless interoperability of services and implementation of short and long codes for public services across multiple service providers. The proposed mechanism shall be established and managed by the Department of Information Technology, Government of India.

Guidelines for Delivery Channels for Provision of Public Services through Mobile Devices

The Objective is to provide:

a. **Guidelines to deliver public services round-the-clock to the users using m-Governance**

b. **Guidelines to develop standard based mobile solutions**

c. **Guidelines to integrate the mobile applications with the common e-Governance infrastructure**

As part of the initiative a shared technical infrastructure **Mobile Services Delivery Gateway (MOBILESEVA)** has been created to enable integration of mobile applications with the common e-Governance infrastructure and delivery of public services to the users.

The objective of creating the MOBILE SEVA is to put in place government-wide shared infrastructure and services to enable rapid development, mainstreaming and deployment of m-Governance services. It will enhance interoperability across various public services as well as reduce the total cost of operation of m-Governance services by providing a common pool of resources aggregating the demand for communication and e-Governance services, and act as a platform for various Government Departments and Agencies to test, rapidly deploy, and easily maintain m-Governance services across the country.

MSDP (Mobile e-governance Services Delivery Platform) provides an integrated platform for delivery of government services to citizen over mobile devices using Mobile Service Delivery Gateway (MSDG), SMS Gateway, m-App Store, m-Payment Services, Location Based Services (LBS), Unstructured Supplementary Services Data (USSD), Unstructured Supplementary Service Notify (USSN), Unstructured Supplementary Service Request (USSR), MMS, Cell Broadcasting Service (CBS), SIM Toolkit (STK), IVRS etc.

MSDG is a messaging middleware to facilitate e-Governance services delivery based on e-Governance Standard protocols which are IIP (Interoperability Interface Protocol), IIS (Interoperability Interface Specifications), IGIS (Inter-Gateway Interconnect Specifications) and Gateway Common Services Specifications (GCSS).

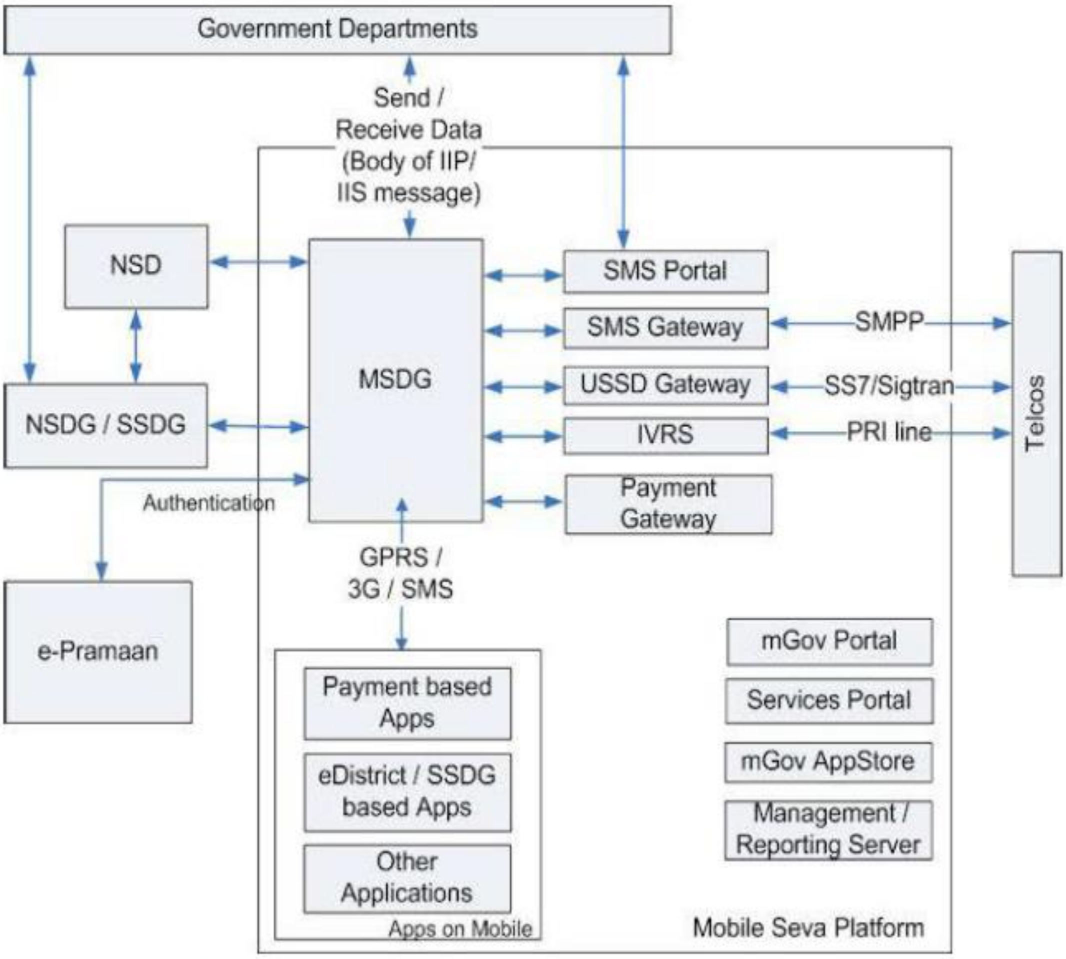


Figure 1: Mobile e-governance Services Delivery Platform (MSDP)

Mobile Application (m-Apps)

Mobile application software is applications software developed for handheld devices, such as mobile

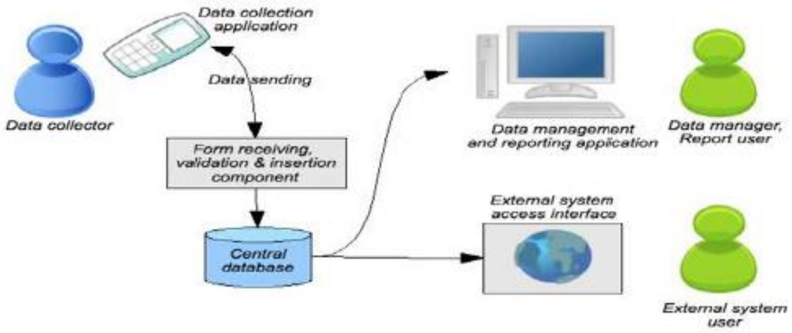
phones, tablets etc. These applications can be pre-installed on phones during manufacture or downloaded by users from various mobile software distribution platforms, or delivered as web applications using server-side or client-side processing (e.g. JavaScript) to provide an application like experience within a Web browser.

1. **Mobile Application Dependency on Handset and O/S**

   Mobile Application software developers also have to consider a lengthy array of screen sizes, hardware specifications and configurations because of intense competition in mobile software and changes within each of the platforms.

2. **Data Collection: m-forms**

   Mobile Application can also make use of the various forms for data collection. Many data collection systems are built from existing commercial or open source components, or even come packaged as an end-to-end solution. The components of data collection relate to each other as shown below:


Data collection application
Data sending
Data collector
Form receiving, validation & insertion component
Central database
Data management and reporting application
Data manager, Report user
External system access interface
External system user

The data collection may be done by various methods. Following are the most common types of data collection client applications which may be used:

1. **Fixed format SMS based Forms:** The 'client application' in this case is the phone's built-in SMS functionality. The user writes and sends SMS in a predefined format, representing answers to successive questions.

2. **Java Micro Edition Platform (J2ME) Application based Forms:** A J2ME application is written in the Java programming language, and loaded onto the phone over Bluetooth or by downloading the application from the Internet. To use the client application, the data collector navigates through questions in an application on the phone, which collects the answers and submits the completed form to a server.

3. **Mobile Operating System based Forms:** Mobile Operating Systems such as Android, Windows Mobile can also be used for developing native platform-dependent applications which can have various forms for data collection.

4. **Web-based Forms:** The 'client application' for web-based forms is the phone's web browser. The user browses to a website, where the form is published in an optimized format for mobile browsers.

5. **Voice-based based Forms:** The user dials a number and then chooses from options on a menu, useful when there are low levels of literacy among data collectors, or when a system is needed that caters for both landline and mobile phones.

6. **Wireless Internet Gateway (WIG) based Forms:** WIG uses a programming language (Wireless Mark-up Language, or WML) that is internal to almost all SIM cards. The menu definition is easy to write, but the size limit is 1MB, making it difficult to support long menus or multiple languages.

7. **Unstructured Supplementary Service Data (USSD) based Forms:** This is a real-time question-response service, where the user initiates a session and is then able to interact with

the remote server by selecting numeric menu options. The phone needs to be continuously connected during the session, which needs a good, consistent signal.

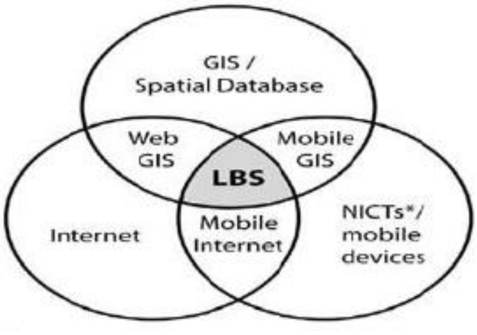
Once data has been captured on the phone, the completed form generally needs to be submitted to a central back-end server.

Other Mobile Technologies

1. Location Based Services (LBS)

Location-based services (LBS) denote services offered to mobile users according to their geographic location. LBS give the possibility of a two way communication and interaction. Therefore the user tells the service provider his actual context like the kind of information he needs, his preferences and his position. This helps the provider of such location services to deliver information tailored to the user needs. LBS enable to retrieve and share information related to their current position. For e.g. Google Latitude.

It works as an intersection of the following features in a system:



***NICT – New Information and Telecommunication technologies**

Geographical Information System (GIS) is a hardware, software and procedures designed to support the capture, management, manipulation, analysis, modelling and display of spatially referenced data for solving complex planning and management problems.

Internet is used to utilize the database dynamically so as to provide the appropriate service.

Mobile Devices as an end- device to execute the service.

2. Cell Broadcast Centre

Cell Broadcast is a mobile technology which allows text messages to be broadcasted to all mobile handsets and similar devices within a designated geographical area.

It is a one-to-many geographically focused service, in contrast to SMS which is a one-to-one or one-to-few service. It is usually used for providing location-based services, especially emergency services, as it utilizes minimum network resources for message broadcast and provides instantaneous delivery to all subscribers in a geographic area.

A Cell Broadcast message is an unconfirmed push service, meaning that the originator of the message does not know who has received the message, allowing for services based on anonymity. Mobile telephone user manuals describe how the user can switch the receiving of Cell Broadcast messages on or off.

Also known as Short message service-Cell Broadcast (SMS-CB), CB messaging is a mobile technology feature defined by the ETSI's GSM committee and is part of the GSM standard. It is also supported by UMTS, as defined by 3GPP.

a) Localization

Given that only a miniscule segment population in India can read and write English, it is important to deploy local/ regional languages to ensure all-round success of m-Governance initiatives. For detailed guidelines please refer to the Mobile Localization Guidelines.

b) Indian Language SMS

Currently, Indian language SMS services are offered by some operators but unlike the English SMS service, the language service is not necessarily interoperable across networks and cannot be availed on all types of handsets. The lack of a standard for Indian SMS comes in the way of providing scalable, interoperable and affordable SMS services in Indian languages.

To realise the goal of interoperable and affordable Indian language SMS, the following are the priority areas:

i. **Text entry standards (i.e. keypad)**
ii. **Encoding standards to support all the major Indian languages**
iii. **Font support standardization for handsets to send and receive Indian language SMS**

i. Text entry methods

The two methods in vogue are:

a. **Mapping the Indian language characters on the handset keypad**

b. **Screen-assisted text inputting mechanisms available from a few OEMs and vendors**

The keypad for the English language has been standardized by ITU. Although efforts on supporting the Indian languages on handheld devices are on, acceptable standards are yet to be evolved. In the absence of any national standards specifying mapping of the Hindi (and other Indian Languages) alphabets to the 12-key mobile devices, the handset vendors keen on penetrating the large Indian market are using their own mappings (which can differ across vendors).

ii. Encoding standard

The Unicode standard supports the 22 major Indian languages but uses more bandwidth (2 octets for each character) and hence the maximum size of SMS that can be sent using Unicode (70 characters) would be less than half of that of an English language SMS (170 characters).

iii. Font Support

Solutions for aesthetic display of Indian language scripts on small handset screens are being worked out. Similarly, solutions are tried out for handsets already in use so that they can receive and display messages in Indian languages, even if they cannot be used to send such messages.

3. Mobile Payment (M-Payment)

Mobile payment is an alternative payment method. Instead of paying with cash, check, or credit cards, a consumer can use a mobile phone to pay for a wide range of services; after having authenticated the user using AADHAR or any other means. The basic aim of mobile payments is to enable micropayments on low-end mobile devices which support only voice and text, in addition to higher end phones which could support web-browsing or Java application capabilities.

a. Mobile banking (M-Banking or mBanking)

M-Banking is a term used for performing balance checks, account transactions, payments, credit applications and other banking transactions through a mobile device. The earlier mobile banking services were offered over SMS, a service known as SMS banking. With the introduction of smart phones with WAP support the mobile web is also being used for M-Banking. Latter with the advancements of web technologies such as HTML5, CSS3 and JavaScript it became feasible to launch mobile web based services to compliment native applications.

b. Immediate Mobile Payment Services (IMPS)

The Immediate Mobile Payment System (IMPS) has been developed by the National Payments Corporation of India (NPCI) to expand the scope of mobile payments to all sectors of the population. IMPS offer an instant, 24X7, interbank electronic fund transfer service through mobile phones.

An IMP provides an inter-operable infrastructure to the banks for enabling interbank real time funds transfer transactions. IMPS rides on the existing NFS Interbank ATM transaction switch infrastructure and message format making it easy for banks to adopt.

To enable the transfer of money, both the sender and the receiver of payment have to link their bank accounts with their phone numbers through their respective banks. The sender has to register for mobile banking service with her/his bank. Upon registration, the bank will provide a link to the Mobile banking software which needs to be installed in the mobile phone to enable payments.

Both the sender and the receiver will receive a Mobile Money Identifier (MMID) while the sender will also receive a Mobile PIN (MPIN) for authentication of transactions. While transacting, the sender has to input the MPIN, receiver’s mobile number and MMID, and the amount of funds to transfer.

IMPS will authenticate the sender, check the receiver’s mobile number and MMID, and transfer the funds to the receiver’s account in real-time. Both the sender and the receiver receive messages notifying them about the success or failure of the transaction.

c. Contactless cards and Mobile Phones

These cards are based upon a technology known as NFC (Near Field Communication) that allows NFC enabled cards to be ready by taping them on or by passing them by, a card reader than swiping them through or inserting into, the POS terminal. They are now being integrated into mobile phone handset for m-Payments.

NFC enabled phones are expected to become more widely available. The NFC chip inside the phone will be connected to the secure element within the SIM card, allowing information stored in an m-wallet to be accessed by the NFC card reader. Authorization for payments involves entering a PIN.

d. Airtime balance for payment

Airtime as balance for payment was realized because of the need for the unbanked majority to easily and cheaply transfer funds around the country. The facility required is the most basic of mobile phones, an account, which can be opened at any one of vendors to start transferring and receiving money.

Since the system uses either SIM toolkit or USSD technology depending on the country, the network charges are minimal to non-existent. It has lowest entry barriers, since it works on more than 95 percent of handsets and has low transaction costs and no bank account or credit card required.

e. Mobile Wallet

A Mobile Wallet is functionality on a mobile device that can securely interact with digitized valuables thereby making payments using the mobile phone. Mobile wallet may reside on a phone or on a remote network / secure server. It is controlled by the user of the wallet.

Using a mobile wallet to make a payment is incredibly simple. When it is time to pay, the user turns on his or her phone’s screen (if the screen is off, when the phone is dormant for instance, the NFC chip will not work), opens the wallet application, enters their pin number, and passes the phone within a few inches of the contactless payment symbol. The payment transaction is then processed just like a conventional card transaction. In addition, relevant offers, discounts, and coupons can be passed from the wallet along with the payment in that same tap of the phone.

4. SIM Application Toolkit

The SIM Application Toolkit is a standard set of commands, under GSM, which defines how the card should interact with the outside world and extends the communication protocol between the card and the handset. It is designed as a client server application.

With SIM Application Toolkit, the card has a proactive role in the handset, i.e., the SIM initiates commands independently of the handset and the network. This enables the SIM to build up an interactive exchange between a network application and the end user and access, or control access to, the network. The SIM also gives commands to the handset such as displaying menus and/or asking for user input.

24.6 Annexure-F (GIGW)

Guidelines for Indian Government Websites

India, the largest democracy in the world, is set to emerge as an ICT Superpower in this millennium. Realising the recognition of 'electronic governance' as an important goal by Governments world over, Indian Government has also laid a lot of emphasis on anytime, anywhere delivery of Government services. As of today, there are over five thousand Government websites in India.

Awareness about the fast changing ICT world and keenness to keep pace with the latest has ensured that almost all the State Governments in India already have their websites up and running. In fact each state has multiple websites belonging to different Departments.

However, these websites follow different Technology Standards, Design Layouts, Navigation Architecture, or, in simple terms, different look and feel as well as functionality.

The need for standardisation and uniformity in websites belonging to the Government cannot be stressed enough, in today's scenario.

As a first step, it is suggested that the Indian Government websites adhere to certain common minimum standards which have been derived, in the form of guidelines discussed in this document, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery. These guidelines could eventually form the basis for establishment of the desired standards.

Compliance to these guidelines will ensure a high degree of consistency and uniformity in the content coverage and presentation and further promote excellence in Indian Government Web space.

These Guidelines have been framed with an objective to make the Indian Government Websites conform to the essential pre-requisites of UUU trilogy i.e. Usable, User-Centric and Universally Accessible. They also form the basis for obtaining Website Quality Certification from STQC (Standardisation Testing Quality Certification) an organisation of Department of Information Technology, Government of India.

These Guidelines are based on International Standards including ISO 23026, W3C's Web Content Accessibility Guidelines, Disability Act of India as well as Information Technology Act of India.

A. Indian Government Entity

All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organisations, States/UTs, District Administrations, and Village Panchayats et al) must prominently display a strong Indian Identity and ownership of Indian Government.

The above objective can be achieved through the following:

1. The National Emblem of India MUST be displayed on the Homepage of the websites of Central Government Ministries/Departments. The usage of National Emblem on an Indian Government website must comply with the directives as per the 'State Emblem of India (Prohibition of improper use) Act, 2005'.

   Further, the State Governments should also display the State Emblem (or the National Emblem in case the State has adopted the National Emblem as its official State Emblem) as per the Code provided in the above Act. The Public Sector organisations and autonomous bodies should display their official logo on the Homepage of the website to re-enforce their identity.

2. The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

3. The lineage of the Department should also be indicated at the bottom of the Homepage and all important entry pages of the website. For instance, at the bottom of the Homepage, the footer may state the lineage information, in the following manner:
   1. This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).
   2. This Website belongs to Department of Industries, State Government of Himachal Pradesh, India' (for a State Government Department).
   3. This is the official Website of Gas Authority of India Limited (GAIL), a Public Sector Undertaking of the Government of India under the Ministry of Petroleum and Natural Gas (for a Public Sector Undertaking).
   4. This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).
4. All subsequent pages of the website should also display the ownership information in a summarised form. Further, the search engines often index individual pages of a website and therefore, it is important that each webpage belonging to a site displays the relevant ownership information.
5. In case of those websites which belong to Inter-Departmental initiatives involving multiple Government Departments which are difficult to list on the Homepage, the Government ownership should still be reflected clearly at the bottom of the page with detailed information provided in the 'About the Portal/Website' section.

6. The page title of the Homepage (the title which appears on the top bar of the browser) MUST be complete with the name of the country included, for instance, instead of the title being just Ministry of Health and Family Welfare, it should state, Government of India, Ministry of Health & Family Welfare.

   Alternatively, in case of a State Government Department, it should state 'Department of Health, Government of Karnataka, India '. This will not only facilitate an easy and unambiguous identification of the website but would also help in a more relevant and visible presence in the search engine results. Further, it is important since the screen readers used by the visually impaired users first read the title of the page and in case the title is not explanatory enough, it may confuse or mislead them.

B. Government Domains

The URL or the Web Address of any Government website is also a strong indicator of its authenticity and status as being official. In today's era with a large proliferation of websites, which resemble Government websites and fraudulently claim to provide reliable Government information and services, the role of a designated Government domain name assumes a lot of significance.

Hence, in compliance to the Government's Domain Name Policy, all Government websites MUST use 'gov.in' or 'nic.in' domain exclusively allotted and restricted to Government websites. The military institutions and organisations in India may also use 'mil.in' domain in place of or in addition to the gov.in /.nic.in domain. The above naming policy applies to all Government websites irrespective of where they are hosted.

Those Departments and Government entities that are using and have been publicising a domain name other than the above should take appropriate early action to register official government domain names and use the existing ones as 'alias' for a period of six months. An intermediary page with a clear message notifying the visitors about the change in the URL and then auto redirecting them to the new URL after a time gap of 10 seconds should be used.

The Domain Name Conventions, as specified in the '.IN Registration' policy should be followed while registering a 'gov.in' Domain Name.

National Informatics Centre (NIC) is the exclusive Registrar for GOV.IN domain names. The use of GOV.IN Domain is restricted to the constituents of Indian Government at various levels right from Central, State/UT, District & Sub-District, block, village etc.

For detailed information and step-by-step procedure on how to register a .GOV IN Domain, one may visit http://registry.gov.in **.**

C. Link with National Portal

1) **india.gov.in:** The National Portal of India is a single window source for access to all information and services being provided by the various constituents of the Indian Government to its citizens and other stakeholders.

There are exclusive sections on Citizens, Business, Overseas, Government, Know India, Sectors etc. catering to the information needs. Sections targeting special interest groups such as Government Employees, Students, Senior Citizens, Kids etc. are also present.

a) **Since the National Portal is the official single entry Portal of the Indian Government, all Indian Government websites MUST provide a prominent link to the National Portal from the Homepage and other important pages of citizens' interest**.

b) **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updating / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

D. Content Copyright

Copyright is a form of protection provided under law to the owners of "original works of authorship" in any form or media. It is implied that the original information put up on the website by a Government Department is by default a copyright of the owner Department and may be copied, reproduced, republished, uploaded, posted, transmitted, or distributed only if the copyright policy of the concerned Department allows so.

Hence, the information, material and documents made available on an Indian Government website MUST be backed up with proper copyright policy explaining the terms and conditions of their usage and reference by others. The copyright policy of a Department could be liberal, moderate or conservative depending upon their preferences based on the kind of information available on their website. However, since it is a duty of a Government

Department to provide all the information in the public domain freely to the citizens, the Departments should aim to have a liberal copyright policy.

The Departments should also be sensitive towards publishing any information having a third party copyright. The Government Departments MUST follow proper procedures to obtain the permission, prior to publishing such information on their websites.

If any published Government Document/Report is being reproduced on any website, whether as excerpts or in full, the source of the same i.e. Full Title of the Report/Document along with the name of the concerned Department and year of publication MUST be provided.

E. Content Hyper linking

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules shouldideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

a) To create a visual distinction for links that lead off site, Cascading Style Sheets (CSS) controls or XSL or some such similar mechanism should be used. In case the link takes the user to another website of the same Department/Ministry/ State, a seamless transition should be used through appropriate CSS controls.

b) Third party content should only be linked when consideration about the copyright, terms of use, permissions, content authenticity and other legal and ethical aspects of the concerned content have been taken into account.

c) The overall quality of a website's content is also dependent, among other things on the authenticity and relevance of the 'linked' information it provides.

d) Further, it MUST be ensured that 'broken links' or those leading to 'Page Not Found' errors are checked on a regular basis and are rectified or removed from the site immediately upon discovery.

F. Privacy Policy

Government websites should follow an extremely cautious approach when it comes to collecting personal details/information about the visitors to the sites. It should be an endeavour to solicit only that information which is absolutely necessary.

In case a Department solicits or collects personal information from visitors through their websites, it MUST incorporate a prominently displayed Privacy Statement clearly stating the purpose for which information is being collected, whether the information shall be disclosed to anyone for any purpose and to whom.

Further, the privacy statement should also clarify whether any cookies shall be transferred onto the visitor’s system during the process and what shall be the purpose of the same.

Whenever a Department’s website allows e-commerce and collects high risk personal information from its visitors such as credit card or bank details, it MUST be done through sufficiently secure means to avoid any inconvenience. SSL (Secure Socket Layer), Digital Certificates are some of the instruments, which could be used to achieve this.

24.7 Annex-G (Open APIs)

Policy on Open Application Programming Interfaces (APIs)

Under the overarching vision of Digital India, Government of India (GoI) aims to make all Government services digitally accessible to citizens through multiple channels, such as web, mobile and common service delivery outlets.

To meet this objective, there is a need for an interoperable ecosystem of data, applications and processes which will make the right information available to the right user at the right time.

Interoperability among various e-Governance systems is an important prerequisite for upgrading the quality and effectiveness of service delivery. For promoting Open Standards for software interoperability across various Government departments and agencies, GoI has already notified the “Policy on Open Standards for e-Governance” and “Technical Standards on Interoperability Framework for e-Governance”.

Open API is the API that has been exposed to enable other systems to interact with that system. Open API may be either integrated with the host application or may be an additional piece of software that exposes any proprietary API with an Open API equivalent. The Open API, whenever possible, may be free of charge and without restrictions for reuse & modifications.

Policy on Open APIs for Government of India” (hereinafter referred to as the “Policy”) will encourage the formal use of Open APIs in Government organizations. This policy sets out the Government’s approach on the use of “Open APIs” to promote software interoperability for all e-Governance applications & systems and provide access to data & services for promoting participation of all stakeholders including citizens.

The objectives of this policy are to:

i. Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.

ii. Enable quick and transparent integration with other e-Governance applications and systems.

iii. Enable safe and reliable sharing of information and data across various e-Governance applications and systems.

iv. Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.

v. Provide guidance to Government organizations in developing, publishing and implementation using these Open APIs.

Government of India shall adopt Open APIs to enable quick and transparent integration with other e-Governance applications and systems implemented by various Government organizations, thereby providing access to data & services and promoting citizen participation for the benefit of the community.

The Open APIs shall have the following characteristics for publishing and consumption:

i. The relevant information being provided by all Government organisations through their respective e-Governance applications shall be open and machine readable.

ii. All the relevant information and data of a Government organisation shall be made available by Open APIs, as per the classification given in the National Data Sharing and Accessibility Policy (NDSAP-2012), so that the public can access information and data.

iii. All Open APIs built and data provided, shall adhere to National Cyber Security Policy.

iv. The Government organizations shall make sure that the Open APIs are stable and scalable.

v. All the relevant information, data and functionalities within an e-Governance application or system of a Government organisation shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.

vi. A Government organisation consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorisation through a process as defined by the API publishing Organisation.

vii. Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.

viii. Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.

ix. The life-cycle of the Open API shall be made available by the API publishing Government organisation. The API shall be backward compatible with at least two earlier versions.

x. All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

xi. Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organisations under the Central Government and those State Governments that choose to adopt this policy for the following categories of e-Governance systems:

- All new e-Governance applications and systems being considered for implementation.
- New versions of the legacy and existing systems.

24.8 Annex-H (Internet of Things)

1. **Sensor & Actuators**
   a. **IEEE 1451**
   IEEE 1451 is a set of smart transducer interface standards developed by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee describing a set of open, common, network-independent communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and control/field networks.
   b. **Identification Technology**
   ISO/IEC JTC 1/SC31 Automatic identification and data capture techniques

   It develops and facilitates standards within the field of automatic identification technologies. These technologies include 1D and 2D barcodes, active and passive RFID for item identification and OCR.

   c. **Domain Specific Compliance:**
   Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, automobile/bus UBS-II (ITS sensor parameter & standards), OBD-II, Electric Vehicle Charging etc.

2. **Communication Technology**
   a. **Thread:**
   Networking protocol called Thread that aims to create a standard for communication between connected household devices.

   b. **AllJoyn:**
   Open source AllJoyn protocol was initially developed by Qualcomm provides tools for the entire process of connecting and maintaining devices on a Wi-Fi network.
   c. **IEEE 802.15.4:**
   It offers physical and media access control layers for low-cost, low-speed, low-power Wireless Personal Area Networks (WPANs).
   IEEE 802.15.4e-2012, IEEE 802.15.4-2011, IEEE 802.15.4-2003, IEEE 802.15.4-2006

   d. **IETF IPv6 over Low power WPAN (6LoWPAN):**
   It defines encapsulation and header compression mechanisms that allow IPv6 packets to be sent to and received over IEEE 802.15.4 based networks.
   6LoWPAN Frame Format
   Fragmentation and Reassembly

Header Compression

Support for security mechanisms

e. **IETF "Routing Over Low power and Lossy (ROLL):**

IPv6 Routing Protocol for Low power and Lossy Networks (LLNs) (RPL)

RPL Topology Formation (Destination Oriented Directed Acyclic Graphs - DODAGs)

RPL Control Messages

f. **IETF Constrained Application Protocol (CoAP):**

It offers simplicity and low overhead to enable the interaction and management of embedded devices.

3. **Use Case/ Application Specific:**

i. **Industrial IoT (IIoT):** Object Modelling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):

- Data Distribution Service (DDS)
- Dependability Assurance Framework For Safety-Sensitive Consumer Devices
- Threat Modelling
- Structured Assurance Case Metamodel
- Unified Component Model for Distributed, Real-Time and Embedded Systems
- Automated Quality Characteristic Measures
- Interaction Flow Modelling Language™ (IFML™)

(Source: http://www.omg.org/hot-topics/iot-standards.htm)

ii. **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modelling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.

iii. **eLearning:** The IEEE Learning Technology Standards Committee (LTSC) is chartered by the IEEE Computer Society Standards Activity Board to develop globally recognized technical standards, recommended practices, and guides for learning technology.

iv. **Intelligent Transportation Systems (ITS):** IEEE has standards activities on many aspects of ITS, such as vehicle communications and networking (IEEE 802 series), vehicle to grid interconnectivity (IEEE P2030.1), addressing applications for electric sourced vehicles and related support infrastructure, and communication for charging (IEEE 1901).

4. **Consortia**

   a. **Open Interconnect Consortium:**

   OIC (Atmel, Dell, Broadcom, Samsung, and Wind River as members) is an open environment to support the billions of connected devices coming online.

   b. **Industrial Internet Consortium:**

   It was founded by Intel, Cisco, AT&T, GE & IBM with the goal of developing standards specifically for industrial use of the Internet of Things.

5. **Architecture Technology**

   a. **IEEE P2413: Standard for an Architectural Framework for the Internet of Things**

   The architectural framework for IoT provides a reference model that defines relationships among various IoT verticals (e.g., transportation, healthcare, etc.) and common architecture elements.

   The standard also provides a reference architecture that builds upon the reference model. The reference architecture covers the definition of basic architectural building blocks and their ability to be integrated into multi-tiered systems.

6. **Further Readings for Standards**

   a. **ITU Standardization Roadmap**

   This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities.It includes Standards/ITU-T Recommendations relatedto Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.

   b. **IERC Position Paper on IoT Standardization:**

   It presents an inventory of existing standards and provides an overview of past and current activity in relation to standardization in the area of Internet of Things, and assembles a series of examples of standardization activities in this area.

24.9 Annex-I (Smart Parking)

The following standards and certifications need to be followed:

1. **Entry Device**
   i. Communication protocol should be TCP/IP
   ii. Conform ISO 9001 Quality Assurance Standard
   iii. CE, FCC, IC, CNRTLUS certified
   iv. Degree of protection based on IEC 60529: IP43
2. **Exit Device**
   i. Conform ISO 9001 Quality Assurance Standard
3. **Entry/Exit Barrier**
   i. The Barrier unit must conform to ISO 9001 Quality Assurance standards
   ii. CE, Ukr - Sepro certified
   iii. Degree of protection: IP34D
4. **Sensors**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP67
5. **Parking light aisle indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP55
6. **Indoor LED indicators**
   i. Conform ISO 9001 Quality Assurance Standard
   ii. Protection Level: IP33
   iii. Communications: Bus RS-485
7. **Other Technical Specifications**

24.10 Annex-J (Public WI-FI)

1. **All equipment must support the following standards/capabilities:**

    i. 802.11n

    ii. 802.11ac

    iii. 802.11e Quality of Service (QoS)

    iv. WMM Wireless Multimedia Extensions

    v. WMM Powersave

    vi. 802.11h Dynamic Frequency Selection and Transmit Power Control

    vii. 802.11i Security, including AES

    viii. 802.1X with dynamic VLAN policies

    ix. WPA2-Enterprise certification

    x. 802.11r Roaming

    xi. preferred: 3X3 MIMO

    xii. preferred: Polycom/SpectraLink VIEW Certification, SpectraLink Voice Priority

    xiii. preferred: Wi-Fi Certified Voice-Enterprise

2. **Wireless Access points specs**

    i. Shall be IEEE 802.11ac compliant concurrent dual radio access point.

    ii. Shall feature a three spatial-stream 802.11ac (3x3 MIMO) integrated or external dual band (2.4GHz & 5GHz) antenna.

    iii. Shall have 802.3af or 802.3at compliant Gigabit PoE UTP port and a console port.

    iv. Shall be IEEE 802.3af PoE compliant and both the radios shall operate at full power and full performance on 802.3af PoE/Gigabit Ethernet.

    v. Shall be Wi-Fi Alliance certified for interoperability with all IEEE 802.11a/b/g/n/ac client devices.

    vi. Shall support up to 16 SSID/VSC profiles.

    vii. Shall support simultaneous detection & prevention of wireless threats on 2.4GHz & 5GHz frequency bands.

    viii. Shall support both centrally managed mode (configured and updated via a controller) and autonomous mode (standalone in the absence of a controller).

    ix. Shall support auto-selection of RF channel and transmit power.

    x. Shall support enforcement of client authorization based on user credentials (802.1X/EAP), and hardware identifiers (MAC address, WEP key).

xi. Shall support ACS or similar feature to reduce co-channel interference (CCI) by automatically selecting an unoccupied radio channel.

xii. Must support Proactive Key Caching and/or other methods for Fast Secure Roaming.

xiii. AP model proposed must be able to be both a client-serving AP and a monitor-only AP for Intrusion Prevention services

xiv. Must support up to 23dbm of transmit power in both 2.4 GHz and 5 GHz radios.

xv. The Wireless AP should have the technology to improve downlink performance to all mobile devices including one-, two-, and three spatial stream devices on 802.11n. The technology should use advanced signal processing techniques and multiple transmit paths to optimize the signal received by 802.11 clients in the downlink direction without requiring feedback and should work with all existing 802.11 clients.

24.11 Annex-H (Disaster Management)

The aim of the local disaster management standards and guidelines is to support local government / municipal corporations to develop a community specific disaster management system, including governance arrangements, a Local Disaster Management Plan (LDMP) using the comprehensive approach to disaster management.

This standard establishes a common set of criteria for all hazards disaster/emergency management with fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity and recovery.

International Standards used in Disaster Warning and Management

S. No.	Standards	Description
1.	ISO 22320:2011	Societal security – Emergency management – Requirements for incident response deals with overall approach for preventing and managing emergencies /disasters
2.	ISO 22322:2015	Societal security -- Emergency management -- Guidelines for Public warning deals with guidelines for developing, managing, and implementing Public warning before, during, and after incidents / disasters
3.	ISO 22324:2015	Societal security — Emergency management — Guidelines for colour-coded alerts deals with guidelines for the use of colour codes to inform people at risk as well as first response personnel about danger and to express the severity of a situation. It is applicable to all types of hazard in any location.
4.	ISO 31000:2009, *Risk management – Principles and guidelines*	It deals with principles, framework and a process for managing risk. It helps organizations / local bodies to increase the likelihood of achieving objectives, improve the identification of opportunities and threats and effectively allocate and use resources for risk treatment.
5.	IEC 31010:2009, Risk management -- Risk assessment techniques	It helps the decision makers understand the risks that could affect the achievement of objectives as well as the adequacy of the controls already in place. It focuses on risk assessment concepts, processes and the selection of risk assessment techniques.
6.	ISO 11320:2011	Nuclear criticality safety -- Emergency preparedness and response
7.	ASCE/SEI 41-06 - *Seismic Rehabilitation of Existing Buildings*	Standards for Seismic retrofitting of existing building including steps to better protect non-structural components (suspended ceilings, non-load-bearing walls and utility systems) and building contents (furnishings, supplies, inventory and equipment)
8.	ISO 19115-1:2014	Defines the schema required for describing geographic information and services by means of metadata. It provides information about the identification, the extent, the quality,

S. No.	Standards	Description
		the spatial and temporal aspects, the content, the spatial reference, the portrayal, distribution, and other properties of digital geographic data and services

24.12 Annexure-K (BIS PIS) as per UBS-II

Specifications for Intelligent Transport System (I.T.S)

Objectives:

1. Harness currently available technologies, with convergence and relevance for the period of the 'Plan' andbeyond.
2. Provide a clear and perceptible upgrade over 2008 specifications incorporating the various feedback of the past implementation.
3. Enhance commuter experience and quality/ substance of visual displays.
4. Make vehicle more driver friendly.
5. Enhance vehicle and customer safety.
6. Improve operating efficiency by reducing variable costs such as fuel, brakes and human resource
7. Increased usability, reliability and life with value for money
8. Standardize, with minimum subjectivity, requirements and responsibilities of various stake holders namely OEMs, purchasers/operators, equipment suppliers, certifying agencies like ARAI and CIRT.
9. Empower purchasers/operators with adequate information and details fortendering
10. Serve as a guideline for purchaser/operator to design ITS based infrastructure at respective control centres and/or depots for enhancing operating efficiencies
11. Define inputs from the bus for 'bus shelter sign' applications (via control centre)
12. Serve as a guideline for 'agencies' like BIS, ARAI, CIRT and ASRTU

Electrical system

Electrical wiring & controls – type

Usability/Functionality/Capability

a Control power supply to and monitor status (voltage, current, faults) of all external and internal fixtures like passenger/driver compartment illumination, fans, buzzer, horn and ITS equipments. Power to ITS equipments will be available even when the engine is not running. This will be provided by putting the "Ignition- ON" Switch followed by switch for ITSequipments

b It should have an inbuilt fault identification, diagnostic and recovery system for theabove

c Receive data from various sensors to assist monitoring vehicle safety/performance features suchas

- **i** Fuel /oil - level/pressure
- **ii** Braking pedalposition
- **iii** Accelerator pedal position and kickdown
- **iv** Brake pad condition and brake pedal temperature (in case of electronically controlled discbrakes)
- **v** Door interlock
- **vi** Kneeling interlock (whereverprovided)
- **vii** Gas leakage detection (whereverprovided)
- **viii** Fire detection/suppression (whereverprovided)

d Diagnostic data from engine and transmission will be provided to VHMD, a minimum list of parameters mentioned is given as per Annex 1 -clause 3,4,5 & 6

- **Architecture-multi 'Node'**

a Each node with its own microprocessor (16 bit minimum)

b Memory (flash minimum 256kb, RAM minimum 64kb, EEPROM minimum128 kb)

c Internal communication on CAN2B

d Outputs suitablefor

- **i** Resistive loads, Coil loads, relay loadsPWM
- **ii** Current measurement, short circuit detection, open load detection and over Current Protection.
- **iii** Digital highside
- **iv** Digital lowside

e Inputs

- **(1)** Analog
- **(2)** Digital high/lowside
- **(3)** for frequency/pulsecounting
- **(4)** For signalamplification

f Each node to be IP54 certified and to comply with test standards under Annex2

- **Primary source of data input to 'SCU' for 'VHMD' via CAN 2B(J1939)**

a. As required under clause 17.5 and Annex1.
b. All ‘CAN’ parameters will be input to SCU in standard format "standardized message name, PGN, SPN andrate

- **ITS enabled bus - On Bus Intelligent Transport System –OBITS**

  - **Architecture**

  a. The architecture defines the overall inter connectivity of the different sub system inside the vehicle, communication within the sub systems and connectivity to the backend solution for the transmission of the real-time vehicle information. It shall consist of following subsystems

  i Passenger information system(PIS)

  ii Automatic vehicle location system(AVL)

  iii Security camera network system(SCN)

  iv Vehicle health monitoring and diagnostics(VHMD)

  On-board pole mounted ticketingmachines

The single control unit ‘SCU’, together with single bus driver console ‘BDC’, form the nucleus of the on- bus vehicle intelligent transport system(OBITS)

  - **PIS System**

  - **Usability/Functionality/Capability**

  a. All drivers related interfaces (input/output/feedback) for PIS must be provided on SCU &BDC

  i The route programming file to be uploaded onSCU

  ii Route selection function is to be provided on BDC

  iii All driver related route information to be displayed onBDC

  Amber coloured, alphanumeric with graphic capability

  b. In-built light sensor with continuously variable brightness control to enable the display intensity to change based on ambient light conditions

  c. Viewing distance

  i Front, side and rear signs 50 meters minimum, for single line text, in day andnight.

  ii Inner 15 meters minimum, for single line text in day andnight.

d. DisplayCharacteristics

i Fixed, scrolling and flashing mode (with fixed route number, up to 6 characters, on front, side and rearsigns).

ii Capability to show customizedgraphics.

iii Two lines English /one line locallanguage.

iv Total display height should accommodate two lines in English language and the Individual heights of each line should be adjustable to enable one line to be larger/smaller than the second line. However, during next stop announcement only single line text isrequired

v It should be possible to display, concurrently, different messages on each of the signs (front, rear, side andinner).

vi It should be able to display special signs like signs for 'PWD enable bus', ‘ladiesspecial’.

e. Signs should have ability to retain the last message displayed in the memory of the sign even in the event of power failure and without the message being reloaded from SCU. Test will be performed by disconnecting the SCU from the sign and power to the sign will be switched ‘off’ and ‘on’ to see if the Last message is retained anddisplayed.

f. Display and voice announcement in English and local languages using Microsoft fonts (or any other as specified in tender) via window based software package (window 7 or latest at the time of inviting thetenders).

g. The system should have a programming capability asunder

i Minimum 75 routes UP and DOWN (150 numbers of destinations) on front, side and rear signs.

ii GPS triggered next stop display on Inner sign with synchronized voice announcement for minimum 75 stops on eachroute.

iii The inner sign should be able to display and announce up to three languages, one after the other in sequence. For example, make display and announcement in English, then Hindi to be followed by local language for benefit of the passengers. Display and announcements should be possible "before arrival" of the bus at the bus stop, "on arrival" of the bus at bus stop and "after departure" of the bus from the busstop.

iv In event of GPS failure, the above functionality should be possible through manual intervention onBDC.

v Display driver and conductor ID once in between the stops on Innersign

vi Inner sign should be able to display text and customized graphics and announce up to pre-recorded messages by driver selecting 1~9 on BDC display panel of thecontroller.

vii Display customized graphics plus synchronized voice announcement – location based

viii Functionality of Display 'clock'-GPS based or 'Default Messages' on Innersign

ix Emergency 'stop' request function- by pressing an emergency switch placed anywhere in the bus the inner sign should display 'stop' message and buzzer located near the driver makes the sound alerting the driver to stop the bus.

h. Two-way communication with central control centre(CCC) viaSCU

- It should be possible to change/choose/select a 'route' remotely over the air from back office and provide current route information to back office
- It should be possible to transmit adhoc messages (English) from back office to internal sign.
- Back office should be able to check, via SCU, the version of firmware loaded on the signs.

i. Sign should be able to store 'diagnostic trouble codes' (DTC)','parameters identifiers (PID) as per Annex 3 and data should be retrievable through SCU.

j. To comply with test standards under Annex2

- **Dimensionsand technical specifications of destination signs**

a. Display size

i Front minimum 200x1800 mm –one

ii Rear and side: minimum 200x900 mm-oneeach

iii Inner: minimum100x800 mm –one

iv For Articulated buses 1 front, 2 inner, 2 side sign and one rear will be employed.

v For mini and midi buses one sign in front of size minimum 200X900 mm and one inner sign minimum100x800mm

b. Pitch

i Front- maximum. H 13.4 mm x V14.1 mm (maximum H10.5 mm x V 14.1mm for mini/midibuses)

ii Side and rear maximum. H10.5 mm x V14.1mm

iii Inner 8 x 8 mm maximum.

c. LED and display quality front, side and rearsigns

i Amber coloured LED, dominant wave length 591~595nm (colour matched and bin graded).

ii UV resistant, diffused lens 4 mm (minimum) or 'SMT PLCC2 standard package'

iii Wide viewing angle 120^{o} horizontal & 60^{o}Vertical

iv Ensure enhanced readability with full clarity on scrolls and long life usage by incorporating non multiplexed system (constant current drive circuit) with typical LED Intensity 400~700 mCd at If =20 mA, alternatively multiplexed design (maximum 4:1) with typical LED intensity 950~1150 mCd at 20ma

d. LED and display quality innersign

i LED amber dot matrix viewing angle 45^{o} all around, intensity minimum 40 mCd, dominant wave length 590 ~595nm

e. Structure

i Front, side and rear signs : light weight structure with toughened glass fixed with UV resistant adhesive infront

ii Inner sign: light weight structure with poly glass /acrylic/toughenedglass.

iii Electronic devices used to be 'automotive grade' rated for temperature -25^{o}C to +85^{o}C (so as to meet tests specified in Annex 2) with conformal coated PCB boards

iv Power to signs shall be supplied through bus multiplex wiring system

- **Automatic vehicle location (AVL) system**

SCU will transmit raw GPS data, of vehicle locations, in NMEA protocol , to back office control centre at user configurable frequency (5 seconds or less),via 3G(GSM)/GPRS, for further processing and use ,including that for signs on bus stops ,BRTS and busterminals.

- **Security camera network (SCN) system**

Usability/Functionality/Capability

a. The Network surveillance system shall consistof

i High resolution cameras, two numbers to monitor bus interiors (doors, driver zone, ticketing zone etc.) and one reversing surveillance camera. For midi/mini buses 1 ambient and 1reversing and for articulated buses 3 ambient and 1 reversing camera to beemployed.

ii Capability of 48-hour recording of images in 'CIF' mode (no sound) for total of four cameras. The recording will be overwritten if not down loaded after the memory is fullyutilized.

iii Capability to transfer the recordings to control centre/depot through SCU via high speed WLAN network (with back haul), in compressedformat

iv Capability to transfer the recordings using SD-card (if provided-refer 17.4.2 a below), tagged to vehicle ID, which is physically removed and transferred to a card reader attached to the depot server.SD card will be provided in a lockablecompartment.

v Capability to transfer recording usingUSB

b. Recording functionalities

i Continuous or schedule basedrecording

ii Event based recording triggered by SCU(VHMD).

iii Event based recording triggered by sensors connected to the 'recorder'(if provided separately)

iv Disconnected cameradetection

v Auto shut down delay after ignition switchoff

vi Auto reset after powerbreak

vii Built inclock

viii Emergency operation: when activated by a foot operated micro pedal switch, the recording will take place at a preselected resolution and FPS.

c. SCU should be able to display on BDC one or more cameras at the same time up to maximum 4.

d. BDC to display only reversing camera picture when reverse gear is engaged.

- **Architecture**

a. 'Recording functionality' could be provided in a 'separate box (recorder)' or alternatively could be in-built into SCU in which case hard disc will be used instead of SD card for storage. The choice will be of the equipment supplier
b. Power supply to 'recorder' will be provided through the bus multiplexing system.
c. Power supply (12V regulated) to camera will be provided from 'Recorder'.

Through the bus multiplexing system when 'recording functionality' is provided in SCU

- **Specifications**

a. 'Camera'specifications

i Fixed lens 3.6mm

ii Picture resolution up to 752 H x 582 V(PAL),

iii Resolution = 420 TV lines minimum,

iv Picture sensor =1/3" CCD or better,

v IR distance 10 meters minimum,

vi Automatic backlightcompensation

vii Ingress protection rating IP66minimum

b. 'Recorder'specifications

i 4 Channelminimum

ii Recording resolutionPAL

(1) CIF (352X288)up to 25 fps maximum each of 4channels

(2) D1 (704X576) up to 25 fps maximum -one channels only

(3) DI (704X576) up to 12 fps maximum each of 4 channels,

iii Stream standards: ISO 1449, video compression standard H.264.

iv 48 hour (for total 4 channels) recording of images and voice in CIF mode.

- **Alternate system**

IP (internet protocol) digital camera using 'network recording' is also permitted with equal or better specifications.

- **Vehicle health monitoring and diagnostics (VHMD)**

17.0.2 'SCU' will receive vehicle health diagnostic data from multiplexing nodes and PIS signs

a The data from multiplexing nodes, on a single CAN 2B(JI939) bus will include parametersfrom

i Vehicle electrical system powered through multiplexing nodes

ii Vehicle safety and performance features

iii Engine and transmission

The list of such parameters is as per Annex 1. All 'CAN' parameters will be receivable in standard format "standardized message name, PGN, SPN and rate.

b The data from PIS signs will include parameters specified in Annex3

17.0.3 'SCU' should be able to create log files and communicate to control centre at end of the day via WLAN the data related to parameters in Annex 1. The log files will be overwritten if not downloaded.

17.0.4 SCU should be able to communicate to control centre, in case any of the parameters listed in Annex 1, exceed a predefined value at any time . Such warning will also pop up real time on BDC screen. The number of such prompts will be five (maximum) at anytime.

17.0.5 SCU should be able to display following parameters on BDC for viewing by driver/workshoptechnician.

a Engine oil pressure, engine coolant temperature, engine speed in RPM, vehicle speed.

b Transmission output shaft speed, transmission input shaft speed, transmission current gear, transmission oil filter restriction switch, transmission oil life remaining, transmission service indicator, transmission sump oil temperature, transmission oil level high / low, hydraulic retarder oiltemperature

c 'Nodes' output status-parameters to be pre agreed at the time oftender.

d Vehicle performance/safety features such as brake condition ,door Interlock ,Kneeling interlock (wherever specified), gas leakage detection (wherever specified), fire detection and suppression (wherever specified).The responsibility of providing requisite sensors for such parameters rests with the OEM.

e Any other engine, transmission diagnostic data –parameters to be pre agreed at the time oftender.

17.0.6 SCU should be able to communicate to control centre, in real time, a pre selected 5 parameters (out of those mentioned above in 17.5.4).

- **On board hand held ticketing machine with smart card**

17.0.7 Specifications

a As per MOUD letter k/14011/28/2009-metro (PT) dated 9thmay2012.

b No compatibility required with SCU andOBITS

- **On board pole mounted smart card ticketing terminals**

17.0.8 Specifications

a Two numbers, one each at two gates system. Specifications as per as per MOUD letter k/14011/28/2009-metro (PT) dated 9th may2012.

17.0.9 Architecture

a SCU should be able to provide route, GPS information in XML format over TCP socket to ticketingmachine.

b Ticketing machine should be able to connect through Ethernet port to enable it send information via the gateway on SCU. All such transmission between ticketing machine and depot/CCC has to be 'secured' at the origin. Purchaser/operator shall make necessary arrangement for identifying ticketing equipment and the protocol to be interfaced.

17.0.10 SCU and BDC architecture Usability/Functionality/Capability a Integrate and interface all featuresof

i Passenger information system(PIS)

ii Automatic vehicle location system(AVL)

iii Security camera network system(SCN)

iv Vehicle health monitoring and diagnostics(VHMD)

b Provide the driver/user interface/display on BDC as specified elsewhere in thisdocument

c Display camera images on BDC as specified elsewhere in this document

d Control PIS functionality as specified elsewhere in thedocument

e Providetwo-way voice and data link with control centre to communicate data and information as specified else where in this document.

The link will be based on open public communications network services 3G (GSM) with downward compatibility with 2G

- f Provide wireless LAN (WiFi) interface for wireless communications between the vehicle and depot network as specified elsewhere in this document. This interface will not be available to passengers.
- g Provide capability to upload firmware/ software and configuration of parameters on 'SCU' via the wireless LAN
- h Provide audio interface to the driver's microphone and earpiece or speaker using wired link to SCU (Telephone dial up is not envisaged)
- i BDC ,on a selectable 'menu' will have 'panic' options' for communicating pre configured messages to controlcentre
- j Capability to store 'diagnostic trouble coded' (DTC)' ,'parameters identifiers (PID) as per Annex3
- k To comply with test standards under Annex2

Technical specifications: SCU

- a Processor : 32/ 64bit
- b Operating system: embedded Windows/Linux with programming software (Windows 7 or latest at the time of calling thetenders)
- c Memory : flash: 2 GB minimum, RAM 512 MB minimum (RAM memory includes SCU andBDC)
- d Interface : CAN 2.0, RS 485,RS 232, fast Ethernet, USB, digital outputs, digital/Analog inputs, WLAN, audio input output,, amplified audio output
- e Interface protocols :as specified elsewhere in this document
- f In built GPS and 3G(GSM)modules
- g WLAN
- h Combi antenna using RG174 cable. The connectors on Combi antenna will be preferably SMA(M) ST plug type for GPS and FME(F) jack type 1/4"-36UNS-2B for3G
- i In built /external two channel amplifier minimum 10 Watts rms each suitable for 4 ~8 Ohm impedance with input for external microphone

j In-built MP3 files storage/playbackfunction.

k Power to SCU & BDC will be supplied through bus multiplexing wiring system

Technical Specifications: BDC

a. Display

i Size 5.7” diagonal minimum

ii Full colour graphic TFT-640 x 480 dots minimum, capable of showing minimum 20 lines in English.

iii Viewing angle (horizontal) 60°/75° (right/left)/ (vertical) 60°/75° (up and down)

iv Adjustable back lighting

b. Key board :4 keys minimum

17.0.11 Technical specifications: GPS modules

a Rating:22 tracking/66 acquisition minimum

b Tracking sensitivity :-165 dBmtyp

c Navigation sensitivity ; -148 dBmtyp

d Update rate I Hz (configurable to 10Hz)

e Time to first fix cold acquisition 35 seconds typ

f Hot acquisition 1 second typ.

g Navigation accuracy 3M horizontal

Technical specifications: 3G(GSM) modules

a GSM/GPRS SMT quad band and UMTS (3G)

b Temperature range -40°C to+85°C

17.0.12 Technical specifications: ‘Combi’ Antenna

a AMPS 850MHz, GSM900MHz, ISM868MHz, DCS1800MHz, PCS1900MHz, 3G UMTS 2.1GHz, Wifi /Blue Tooth (2.4GHz),GPS

(1575.42MHz). Separate WLAN antenna may be provided if necessary.

b GPRS

i Impedance 50Ohm

ii Radiation pattern Omni-directional

iii Polarization linear(vertical)

c GPS

i Impedance 50Ohms

ii VSWR <1.5:1

iii PolarizationRHCP

d Waterproof IP-66

e Temperature range -40°C to+85°C

f RG174cable

17.0.13 Fitment on bus

a All ‘OBITS’ equipment including wiring harness, antennas to be original factoryfitment.

b Front, side, rear signs should be mounted with a gap with the glass so that the glass on signs and of the bus can be cleaned by wiping

c All equipment should be fitted in a way to minimize unintentional damage, shielded from direct engine heat, protected from water splash anddust.

d All cables need to be properlyanchored

e Others:

i Front sign: central

ii Rear sign: central

iii Side sign: first window ahead of rear door (central line of sign should coincide with central line ofwindow)

iv Inner sign: centralize along the width of bus behind the driver'spartition

v Speakers with protective grill: one each near the doors and others equally distributed across the length of the bus- Total no.4

vi SCU, recorder, amplifier: secured and ventilated compartment right above the driver

vii BDC: ergonomically placed for driverease

viii Camera: as specified elsewhere

ix Ticketing machines - pole Mounted: as specifiedelsewhere

x Combi antenna: suitable place to define inside the bus (preferably) with direct line of view for 'affixing' theunit.

17.0.14 Communication amongst sub systems

a	'Signs'to 'SCU'	RS 485

b	'Multiplexing nodes'to'SCU'	CAN 2B(J1939)
c	'Camera'to 'Recorder’	AVI or Ethernet (for ‘IP’ camera option)
d	'SCUto'BDC' Ethernet/DVI/VGA/HDMI/RS232/RS485 asrequired.	
e	Add -on 'Ethernet switch' and CAN ports arepermitted	

- **Communication between SCU and depot/central control centre (CCC)**

a. **AVL to CCC**:

Raw GPS data in NMEA 0183 protocol (GPVTG, GPGGA, GPRMC, GPGSV and GPGSA) and route number via open public communications network services 3G and download compatibility

b. **VHMD real time warning to CCC**

Open public communications network services 3G and download compatibility

c. **VHMD end of the day to depot**

IEEE 802.11 Wireless LAN (WiFi) via 'Back haul' at depot

d. **SCN 48-hour recording to depot**

IEEE 802.11 Wireless LAN (WiFi) via 'Back haul' at depot plus SD card physical transfer/USB physical transfer

e. **Firmware downloads from Depot**

IEEE 802.11 Wireless LAN (WiFi) via 'Back haul' at depot

f. **PIS Two-way communication to depot need based, API to be pre-agreed**

b Any protocol provided by ITS supplier will be under a 'NDA' amongst the parties

- **Additional requirements of Purchaser/Operator**

a. If required, Purchaser/Operator can specify as a part of their tender requirements, unambiguously, any additional requirement in relation to ‘interface’ with their ITS Infrastructure.

- **TA' and 'COP' approvals**

a. The notified agencies, as under rule number 126 of CMVR, will be responsible for approvals and certification of 'OBITS' system as definedabove.

b. Above approvals, when accorded to sub system suppliers such as PIS, SCU and BDC, etc will be valid across the board for various purchaser/operator, OEMs and tenders

- **Warranties**

a. The standard warranty will be identical to the warranty of bus (up to 3 years maximum) however purchaser/operator may ask OEMs for extended warranty /annual maintenance contract after expiry of standard warranty periods.

- **ITS Infrastructure at Purchaser/Operator**

a Purchasers/Operator(s) are obligated to install the necessary ITS infrastructure and human resource to 'take over' the OBITS system from OEMs and have their own cell for day to day operations and needs. Typical examples being: PIS route programming including voice recordings, maintaining up-to-date LAT LONG database, 'Back Haul'operations.

b OEMs are obligated to provide training to such purchaser/operator(s) staff before delivery of buses.

c **Driver Score Card/Driver rating:** Purchasers/Operator(s) are obligated to make use of the information from OBITS to incorporate a practice of 'Driver Score Card'. A few suggested parameters are

i. Door Open whiledriving
ii. HarshAcceleration
iii. Excessive Idling
iv. Harsh Braking
v. Overrevving
vi. Overspeeding
vii. Excessive Trip Mileage (FuelMileage)
viii. Non-Adherence to 'Trip Schedule' e.g. 'Late Start', 'Off Route' and 'Duty Cycle'
ix. Driving with Faults: Warning Pop ups reported and initiative to getcorrected
x. Panic Buttonusage
xi. Cameras switchedoff
xii. Internal Sign Switched off Data from the above will be based on
    - VHMD Log files and SCN data downloaded at end of the day including Driver ID
    - Live AVL location transmitted from Bus.

ASCDCL

Aurangabd Smart City
development corporation ltd