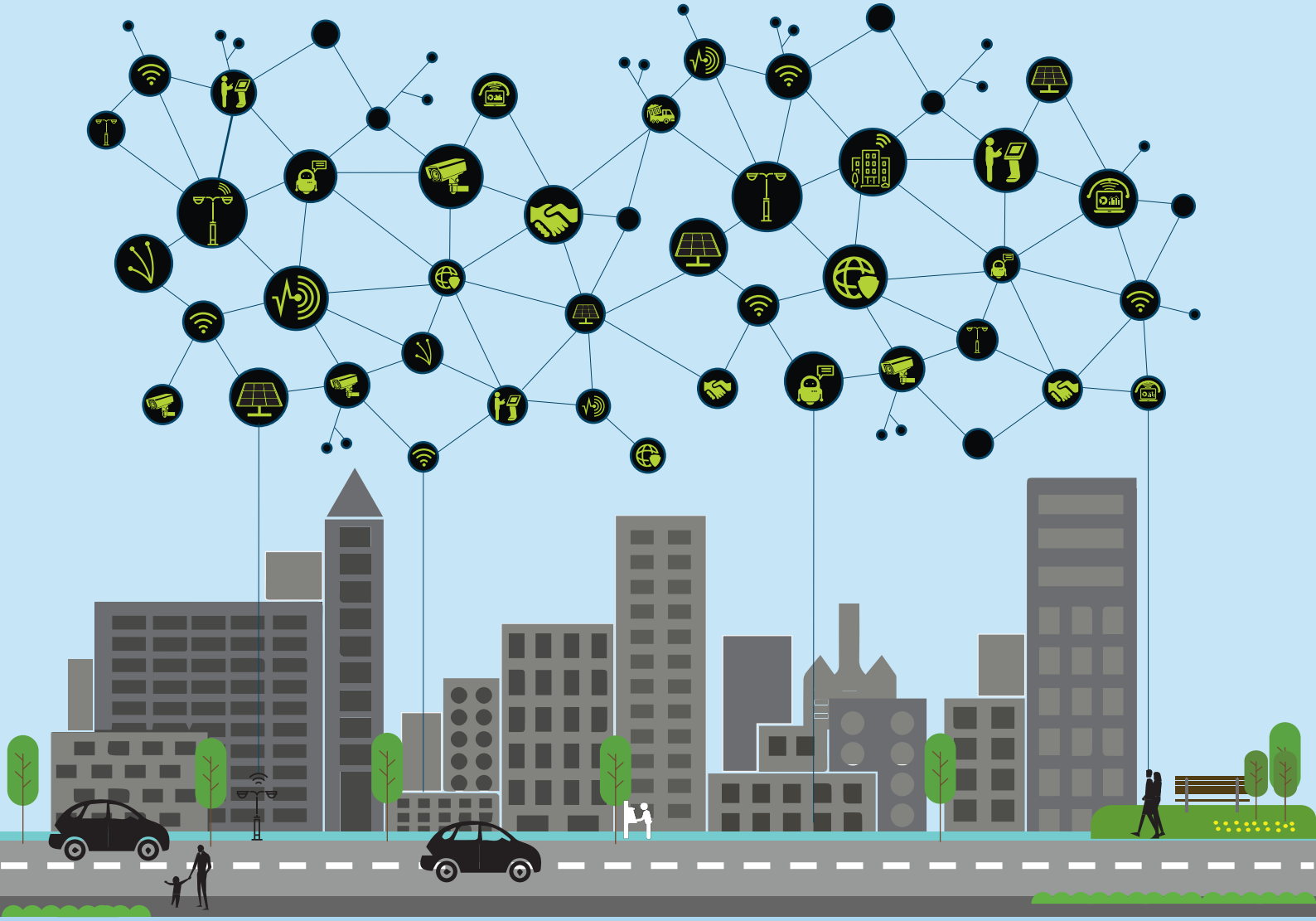
REQUEST FOR QUALIFICATION (RFQ)
CUM
REQUEST FOR PROPOSAL (RFP)



REF. No. : AITL/SBIA/2018-19/03

APPOINTMENT OF MASTER SYSTEM INTEGRATOR (MSI)
FOR
SUPPLY, IMPLEMENTATION, INTEGRATION, OPERATIONS AND MAINTENANCE OF SMART CITY ICT COMPONENTS AT BIDKIN PHASE-1 AREA OF AURIC

VOLUME III : TERMS OF REFERENCE

DECEMBER, 2018

AURANGABAD INDUSTRIAL TOWNSHIP LIMITED (AITL)

UDYOG SARATHI, MIDC OFFICE, MAROL INDUSTRIAL AREA
ANDHERI (EAST), MUMBAI, MAHARASHTRA, INDIA - 400093

Aurangabad Industrial Township Limited

International Competitive Bidding (ICB)

APPOINTMENT OF MASTER SYSTEM INTEGRATOR (MSI)

FOR

SUPPLY, IMPLEMENTATION, INTEGRATION, OPERATIONS AND MAINTENANCE OF SMART CITY ICT COMPONENTS AT BIDKIN PHASE-1 AREA OF AURIC

AURANGABAD INDUSTRIAL TOWNSHIP LIMITED (AITL)

REQUEST FOR QUALIFICATION (RFQ)

CUM

REQUEST FOR PROPOSAL (RFP)

Volume III – Terms of Reference

(Ref No: AITL/SBIA/2018-19/03)

December, 2018

Aurangabad Industrial Township Limited

(AITL)

Udyog Sarathi, MIDC Office, Marol Industrial Area
Andheri (East), Mumbai, Maharashtra, India – 400093

Table of Contents

Table of Contents

Abbreviations

Abbreviation	Definition
AAA	Authentication, Authorization and Accounting
ACC	AURIC Control Centre
ACL	Access Control List
ADC	Application Delivery Controller
ADF	Automatic Document Feeder
AEE	AURIC e-Governance and ERP
AES	Advanced Encryption Standard
AGC	Automatic Gain Control
AGP	Advanced Graphics Processor
AITL	Aurangabad Industrial Township Limited
AIX	Advanced Interactive eXecutive
AMC	Annual Maintenance Contract
AMD	Advanced Micro Devices
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
ANPR	Automatic Number Plate Recognition
ANSI	American National Standards Institute
AP	Access Point
API	Application Program Interface
AQI	Air Quality Index
ARIA	Accessibility Initiative – Accessible Rich Internet Applications
ASC	Auto Signal Compensation
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers
ASICS	Application-Specific Integrated Circuit
ASTM	American Society for Testing and Materials
ATCC	Automatic Traffic Counting & Classification System
ATI	Advanced Technology Institute
ATM	Automated Teller Machine
ATP	Acceptance Testing Procedure
AURIC	Aurangabad Industrial City
AVC	Advance Video Coding
AVI	Automatic Vehicle Identification
AVL	Automatic Vehicle Locator
AWG	American Wire Gauge
AWS	Amazon Web Services
BAC	Building Automation and Control
BEE	Bureau of Energy Efficiency
BGP	Border Gateway Protocol
BIFMA	Business and Institutional Furniture Manufacturers Association

Abbreviation	Definition
BIS	Bureau of Indian Standards
BMS	Building Management System
BOOTP	Bootstrap Protocol
BRS	Business Requirement Specifications
BSSID	Basic Service Set Identifier
BYOD	Bring Your Own Device
CAD	Computer Aided Dispatch
CAPI	Common Application Programming Interface
CATV	Cable TV
CBR	Constant Bit Rate
CCTV	Closed Circuit Television
CDRW	Compact Disc Re-Writable
CFC	Citizen Facilitation Centre
CFR	Code of Federal Regulations
CIF	Common Intermediate Format
CIFS	Common Internet File Service
CISPR	Comité International Spécial des Perturbations Radioélectriques
CKC	CISCO Kinetics for Cities
CLI	Caller Line Identification
CMDB	Configuration Management Database
CMOS	Complementary Metal-Oxide Semiconductor
CNAME	Canonical Name
COTS	Commercially Available Off-The-Shelf
CPS	Connections Per Second
CPU	Central Processing Unit
CRM	Customer Relationships Management
CSA	Canadian Standards Association
CSV	Comma Separated Values
DBMS	Database Management System
DCMS	Display Content Management System
DDOS	Distributed Denial of Service
DDS	Digital Display Screen
DES	Data Encryption Standard
DFC	Dedicated Freight Corridor
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual In-Line Memory Lane
DIN	Deutsches Institut für Normung
DIPP	Department of Industrial Policy and Promotion
DLP	Defect Liability Period
DLPTM	Digital Light Processing
DMIC	Delhi Mumbai Industrial Corridor
DMICDC	Delhi Mumbai Industrial Corridor Development Corporation

Abbreviation	Definition
DNS	Domain Name Service
DNSSEC	Domain Name System Security Extensions
DOB	Date Of Birth
DOD	Depth Of Discharge
DOS	Days Of Service
DOT	Department of Telecom
DPI	Deep Packet Inspection
DPR	Detailed Project Report
DRBG	Deterministic Random Bit Generator
DRP	Disaster Recovery Plan
DSA	Digital Signature Algorithm
DSS	Data Security Standard
DVD	Digital Video Disc
DVI	Digital Visual Interface
DVM	Digital Video Manager
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECB	Emergency Call Box
ECBC	Energy Conservation Building Code
ECC	Error Connecting Code
ECDH	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EIA	Electronic Industries Alliance
EIRP	Effective Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMS	Enterprise Management System
EPABX	Electronic Private Automatic Branch Exchange
EPC	Engineering, Procurement and Construction
EPS	Encapsulated PostScript
ERP	Enterprise Resource Planning
ESD	Electrostatic Discharge
FAQ	Frequently Asked Questions
FAT	Factory Acceptance Test
FCC	File Client Cache
FDMS	Fibre Distribution Management System
FIPS	Federal Information Processing Standard
FOSC	Fibre Optic Splice Closure
FRC	Fibre Reinforced Concrete
FRP	Fibre Reinforced Plastic
FRS	Functional Requirements Specifications
FTP	File Transfer Protocol

Abbreviation	Definition
FTTX	Fibre-to-the-X
GDP	Gross Domestic Product
GIS	Geographic Information System
GPI	General Purpose Interface
GPO	Group Policy Object
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
HBA	Host Bus Adapter
HDD	Horizontal Directional Drilling
HDMI	High-Definition Multimedia Interface
HDPE	High-Density Polyethylene
HIPS	Host Intrusion Prevention System
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
HUDCO	Housing and Urban Development Corporation Limited
HVAC	Heating, Ventilation and Air Conditioning
IAT	Installation Acceptance Test
ICA	Independent Computing Architecture
ICB	International Competitive Bidding
ICEA	Insulated Cable Engineers Association
ICES	Interference-Causing Equipment Standard
ICMP	Internet Control Message Protocol
ICT	Information & Communications Technology
IDS	Intrusion Detection System
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IES	Illuminating Engineering Society
IGMP	The Internet Group Management Protocol
IIFCL	India Infrastructure Finance Company Limited
IIS	Internet Information Services
IMAP	Internet Mail Access Protocol
IP	Ingress Protection
IPFIX	Internet Protocol Flow Information Export
IPI	Infrastructure Provider Category I
IPS	Intrusion Prevention System
IPSEC	Internet Protocol security
IRIG	Inter-Range Instrumentation Group

Abbreviation	Definition
ISA	Industry Standard Architecture
ISDN	Integrated Services Digital Network
ISI	Indian Standards Institute
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
ITS	Intelligent Transportation System
ITU	International Telecommunication Union
IVRS	Interactive Voice Response System
JBIC	Japan Bank for International Cooperation
JCA	Java EE Connector Architecture
JCE	Java Cryptography Extension
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
KCDSA	Korean Certificate-based Digital Signature Algorithm
KPI	Key Performance Indicator
KVM	Keyboard, Video and Mouse
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCD	Liquid Crystal Display
LCV	Light Commercial Vehicle
LDAP	Lightweight Directory Access Protocol
LDPE	Low Density Poly Ethylene
LED	Light Emitting Diode
LIC	Life Insurance Corporation
LiFePO4	Lithium Iron Phosphate
LLDP	Link Layer Discovery Protocol
LMS	Land Management System
LNA	Low Noise Amplifier
LTE	Long Term Evolution
MAC	Media Access Control
MAPI	Messaging Application Programming Interface
MAV	Multi Axle Vehicle
MCB	Miniature Circuit Breaker
MCC	Mini Control Centre
MCU	Multipoint Control Unit
MDF	Medium Density Fibreboard
MDM	Mobile Device Management
MED	Media Endpoint Discovery
MEP	Mechanical, Electrical and Plumbing
MGCP	Media Gateway Control Protocol
MIB	Management Information Bases

Abbreviation	Definition
MIDC	Maharashtra Industrial Development Corporation
MIS	Management Information System
MJPEG	Motion Joint Photographic Experts Group
MOV	Metallic Oxide Varistor
MPEG	Moving Picture Experts Group
MPLS	Multi-Protocol Label Switching
MSI	Master Systems Integrator
MTBF	Mean Time Between Failures
MTR	Main Telecom Room
MTTR	Mean Time To Repair
NABL	National Accreditation Board for Laboratories
NBC	National Building Code
NEC	National Electric Code
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Prevention Association
NFS	Network File System
NIC	Network Interface Card
NIDP	Network Intrusion Detection & Prevention
NLP	Natural Language Processing
NMS	Network Management System
NNTP	Network News Transfer Protocol
NSS	Network Switching System
NTP	Network Time Protocol
NTS	Network Time Server
NVR	Network Video Recorder
NWT	Non Water Tight
OCEF	Optical Cable Entrance Facility
OEM	Original Equipment Manufacturer
OFC	Optic Fibre Cable
ONVIF	Open Network Video Interface Forum
OPS	Open Pluggable Specification
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
OTP	One Time Password
OWASP	Open Web Application Security Project
PAT	Prototype Acceptance Test
PBR	Policy Based Routing
PCAP	Packet Capture
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation
PDF	Portable Document Format
PEAP	Protected Extensible Authentication Protocol

Abbreviation	Definition
PEM	Privacy Enhanced Mail
PFX	Personal Information Exchange Format
PIN	Personal Identification Number
PIT	Pre-Installation Testing
PKCS	Public Key Cryptographic Standards
PKI	Public Key Infrastructure
PLB	Permanently Lubricated
PLR	Persistence Loss Ratio
PMD	Polarization Mode Dispersion
POE	Power Over Ethernet
PoP	Point of Presence
PPM	Parts Per Million
PPP	Public Private Partnership
PRI	Primary Rate Interface
PTR	Pointer
PTZ	Pan Tilt Zoom
PV	Photovoltaic
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RCC	Reinforced Cement Concrete
RDBMS	Relational Database Management System
RFC	Request for Comments
RFP	Request for Proposal
RFQ	Request for Qualification
RGB	Red Green Blue
RHEL	Red Hat Enterprise Linux
RMON	Remote Monitoring
RMU	Ring Main Unit
RoHS	Restriction of Hazardous Substances
ROM	Read Only Memory
RPC	Remote Procedure Call
RPM	Revolutions Per Minute
RPO	Recovery Point Objective
RRE	Remote Reader Electronics
RSA	Rivest, Shamir and Adelman
RTA	Regional Transport Authority
RTC	Real Time Clock
RTF	Rich Text Format
RTI	Right to Information
RTO	Regional Transport Office
RTP	Real-time Transport Protocol
RTSP	Rapid Spanning Tree Protocol

Abbreviation	Definition
SAML	Security Assertion Markup Language
SAS	Statistical Analysis System
SAT	Systems Acceptance Test
SATA	Serial Advanced Technology Attachment
SBIA	Shendra Bidkin Industrial Area
SCADA	Supervisory Control and Data Acquisition
SCCP	Skinny Client Control Protocol
SCP	Security Certified Program/ Smart City Platform
SCSI	Small Computer System Interface
SDHC	Secure Digital High Capacity
SDRAM	Synchronous Dynamic Random Access Memory
SFP	Small Form-factor Pluggable
SHA	Secure Hash Algorithms
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIT	Systems Integration Testing
SLA	Service Level Agreement
SLES	SUSE Linux Enterprise Server
SLG	Street Lighting Gateways
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	System-on-a-Chip
SPA	Special Planning Authority
SPV	Special Purpose Vehicle
SQL	Software Queueing Language
SRS	Software Requirement Specifications
SSD	Solid-State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-On
STP	Spanning Tree Protocol
SUSE	Software and System-Entwicklung
TACACS	Terminal Access Controller Access Control System
TACS	Total Access Communication System
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing

Abbreviation	Definition
TEC	Telecommunication Engineering Centre
TELNET	Teletype Network
TFTP	Trivial File Transfer Protocol
THD	Total Harmonic Distortion
TIA	Telecommunications Industry Association
TPM	Trusted Platform Module
TPS	Transactions Per Second
TRAI	Telecom Regulatory Authority of India
TRD	Test Results Documentation
TSP	Telecom Service Provider
UDP	User Datagram Protocol
UHD	Ultra-High-Definition
UPC	Ultra-Physical Contact
UPI	Unified Payments Interface
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Universal Time Coordinated
UTP	Unshielded Twisted Pair
VAC	Volt AC
VBR	Variable Bit-Rate
VDI	Virtual Desktop Infrastructure
VDM	Video Display Module
VDW	Voice Directed Warehousing
VGA	Video Graphics Array
VLAN	Virtual Local Area Network
VMS	Video Management System
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
WCCD	World Council on City Data
Wi-Fi	Wireless Fidelity
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
XLPE	Cross Linked Polyethylene insulation
XML	Extensible Markup Language
AAA	Authentication, Authorization and Accounting
ACC	AURIC Control Centre

1 Introduction

1.1 Overview

Government of India (GoI) has envisaged the development of Delhi Mumbai Industrial Corridor (DMIC) along the alignment of proposed multi-modal high axle load Dedicated Freight Corridor (DFC) between Delhi and Mumbai. The corridor covers approximately 1483 km and passes through six (6) states. To tap the development potential of the proposed freight corridor, a band spanning 150 km on both sides of the freight corridor has been identified as the 'Influence Region' and is proposed to be developed as DMIC. The multi-billion dollar DMIC is one of the largest infrastructure and economic development programs in India's history.

The Delhi Mumbai Industrial Development Corporation (DMICDC) acts as an intermediary for the purposes of development and establishment of infrastructure projects and facilities in India. It is responsible for developing and disseminating appropriate financial instruments, negotiating loans and advances of all nature, and formulating schemes for mobilization of resources and extension of credit for infrastructure. DMICDC undertakes project development services for investment regions/industrial areas/economic regions/industrial nodes and townships for various central agencies and state governments. The shareholders of DMICDC include different agencies: Government of India represented through Department of Industrial Policy and Promotion (DIPP), Ministry of Commerce and Industry, Japan Bank for International Cooperation (JBIC), Housing and Urban Development Corporation Limited (HUDCO), India Infrastructure Finance Company Limited (IIFCL) and Life Insurance Corporation of India (LIC).

GoI's national Programme "Make-In-India" has the mandate to promote the manufacturing sector in a comprehensive manner. The programme aims to facilitate investment, foster innovation, enhance skill development, protect intellectual property, and build best-in-class manufacturing infrastructure in India. Overall, the contribution of manufacturing sector to the GDP of India is still lower as compared to that of other fast developing economies of countries like Thailand, China, Indonesia and Malaysia. Through this "Make-In-India" Programme, GoI aims to enhance the contribution of manufacturing sector to the country's GDP and aims to surpass the contribution realized in other developing economics. DMICDC with the development of DMIC project plays a key role in realizing this GoI's vision of Make-In-India.

As part of one of the project initiatives undertaken by DMICDC, Shendra-Bidkin Industrial area is being implemented in the state of Maharashtra as a greenfield industrial smart city. Shendra-Bidkin Industrial area, known as Aurangabad Industrial City (AURIC) is being jointly developed between DMICDC and Maharashtra Industrial Development Corporation (MIDC) under the SPV of Aurangabad Industrial Township Limited (AITL).

MIDC is the industrial development arm of the Government of Maharashtra responsible for creating state-of-the-art infrastructure for industrial development in each district of the state and assisting entrepreneurs in setting up industrial units. Within a span of five (5) decades of its inception, MIDC has become the premier industrial infrastructure development agency in India, a powerful engine of progress with a trailblazing record and above all the pride of Maharashtra.

AITL has 51% stake of MIDC and 49% stake of DMIC Trust. AITL will also have the status of a Special Planning Authority (SPA) and will be responsible for development, management and operations of AURIC.

1.2 Project Background

AURIC is strategically located near Aurangabad in Maharashtra. Besides an existing rail and highway network that connects the new city with major cities in India, AURIC is approximately 10 minutes away from Aurangabad International Airport and approximately 30 minutes away from downtown Aurangabad. The Jawaharlal Nehru Port Trust's proposed dry port and container terminal at Jalna is also approximately 40 minutes away. AURIC is planned as an extension of the existing MIDC's Shendra Industrial Park to the town of Bidkin located near Aurangabad.

Aurangabad has significant potential for growth in various manufacturing sectors. The Aurangabad District is already an established location for automobile and automobile related manufacturing. Aurangabad will be the showcase for Maharashtra's strengths in manufacturing and technology — automobiles, textiles, apparel, consumer durables, and green industry. AURIC will be the next sought after trade city, venue for manufacturing-related research and design, and high-tech hub centrally located within the state. The strategic location of the AURIC places it at the convergence of Maharashtra's production, manufacturing, and tourism (historic sites). The industrial area also has the potential to become a niche for meetings, incentives, conventions, and exhibitions.

Development of AURIC has been divided into two (2) phases – Phase-1 is AURIC-Shendra and Phase 2 is AURIC-Bidkin. AURIC-Bidkin spreads across an area of approximately 32 sq. km, while AURIC-Shendra is an 8.45 sq. km area. Currently, the civil development and ICT infrastructure of AURIC-Shendra is under implementation. Concurrently, implementation of Phase-1 of AURIC-Bidkin, comprising of approximately 10 sq. km is also under implementation. With the overall vision of developing AURIC as a smart greenfield industrial city, AITL also has a focus on mixed-use development that includes residential, commercial, public-amenities along with social infrastructure beyond the industrial land use. The overall vision of the project includes implementation of state-of-the-art infrastructure that will be highly reliable, available and integrated over technology. AURIC aims to drive the expansion of Aurangabad as a major industrial hub with an aim to attract and retain a highly skilled workforce and generate over 150,000 jobs as direct employment along with housing over 300,000 people including the industrial workforce and their families. While AURIC-Shendra is growing as a technological hub, AURIC-Bidkin is expected to project itself as the potential hub for defence and manufacturing sector in the state of Maharashtra.

The paradigm shift towards modern cities includes a strong need to have integrated and connected infrastructure with a focus on citizen-centric services. The overall vision of AURIC includes positioning of Information & Communications Technology (ICT) as the key enabler to integrate various functions of the city development and operations, provide advanced and affordable services to the citizens along with efficient governance and management of the city operations. ICT will enable creation of a sustainable eco-system of the government, industries/businesses, social infrastructure with an overall citizen-centric development. It will enable AITL to be an efficient and tech-savvy organization that will truly leverage ICT for its operations and decision making. ICT will cultivate the development of a digital and connected city which ultimately helps in promoting and sustaining economic growth and development. An illustration of the systems that are envisaged as part of the project is presented in Exhibit 1 below:

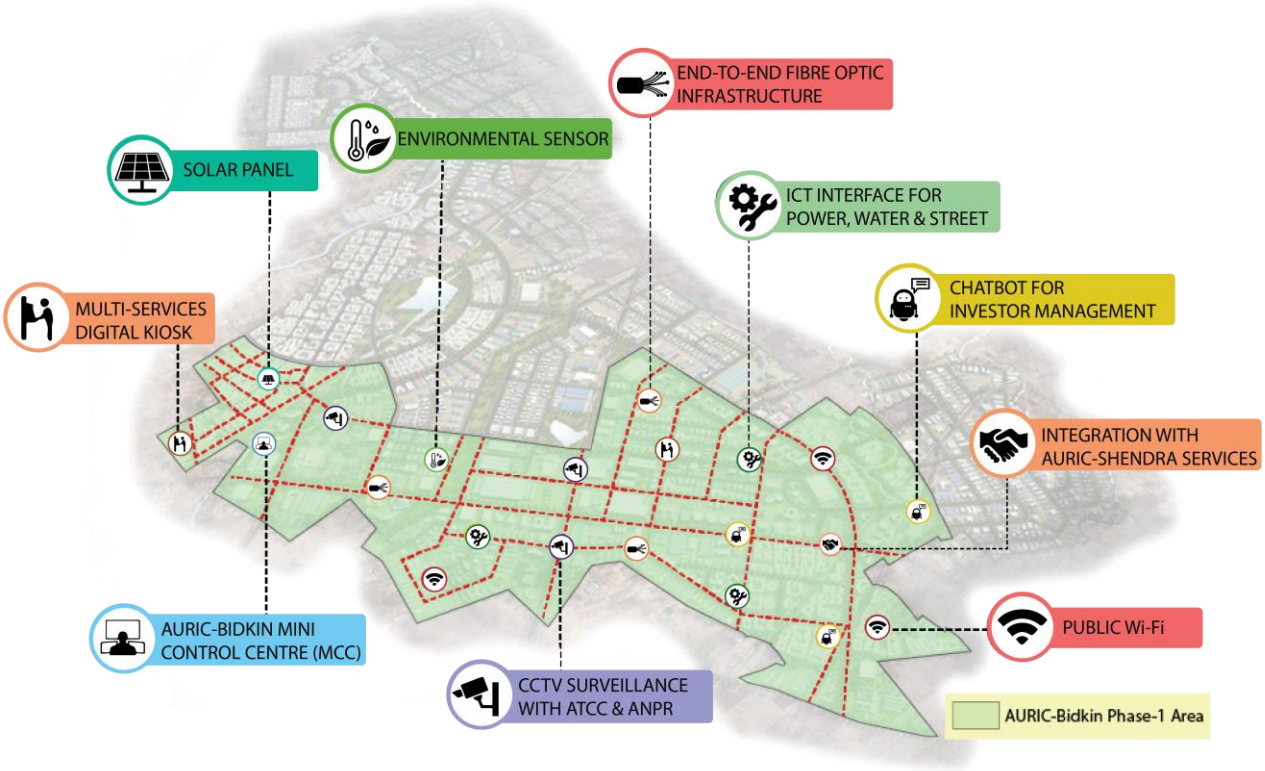


Exhibit 1: Smart City ICT Components

This RFQ cum RFP (Bidding Documents) is for the appointment of a Master System Integrator (MSI) that shall be responsible for supply, implementation, integration, operations and maintenance of smart city ICT components for Bidkin Phase-1 area of AURIC (Project). The MSI shall be responsible for complete turnkey of the system including the design, supply, installation, testing, integration, commissioning, operation and maintenance of the components that are being provided as part of this Project. In addition, it is also envisaged that MSI for AURIC-Bidkin to work in coordination with the MSI of AURIC-Shendra in order to integrate various services of AURIC-Bidkin with the Control Centre in AURIC-Shendra known as AURIC Control Centre (ACC). ACC will act as the common command and control centre for both – Shendra and Bidkin.

The Client has appointed an ICT Consultant for the Bidkin area of AURIC who will be the representative for AITL on this Project. In addition, the Client also has an overall Program Manager for the development of AURIC. EPC Contractors have been appointed for the civil trunk infrastructure, utilities work and the implementation of the Project.

Exhibit 2 below shows the location map of Shendra and Bidkin areas of AURIC. Exhibit 3 and Exhibit 4 shows the projected population and employment for Shendra-Bidkin Industrial Areas respectively.

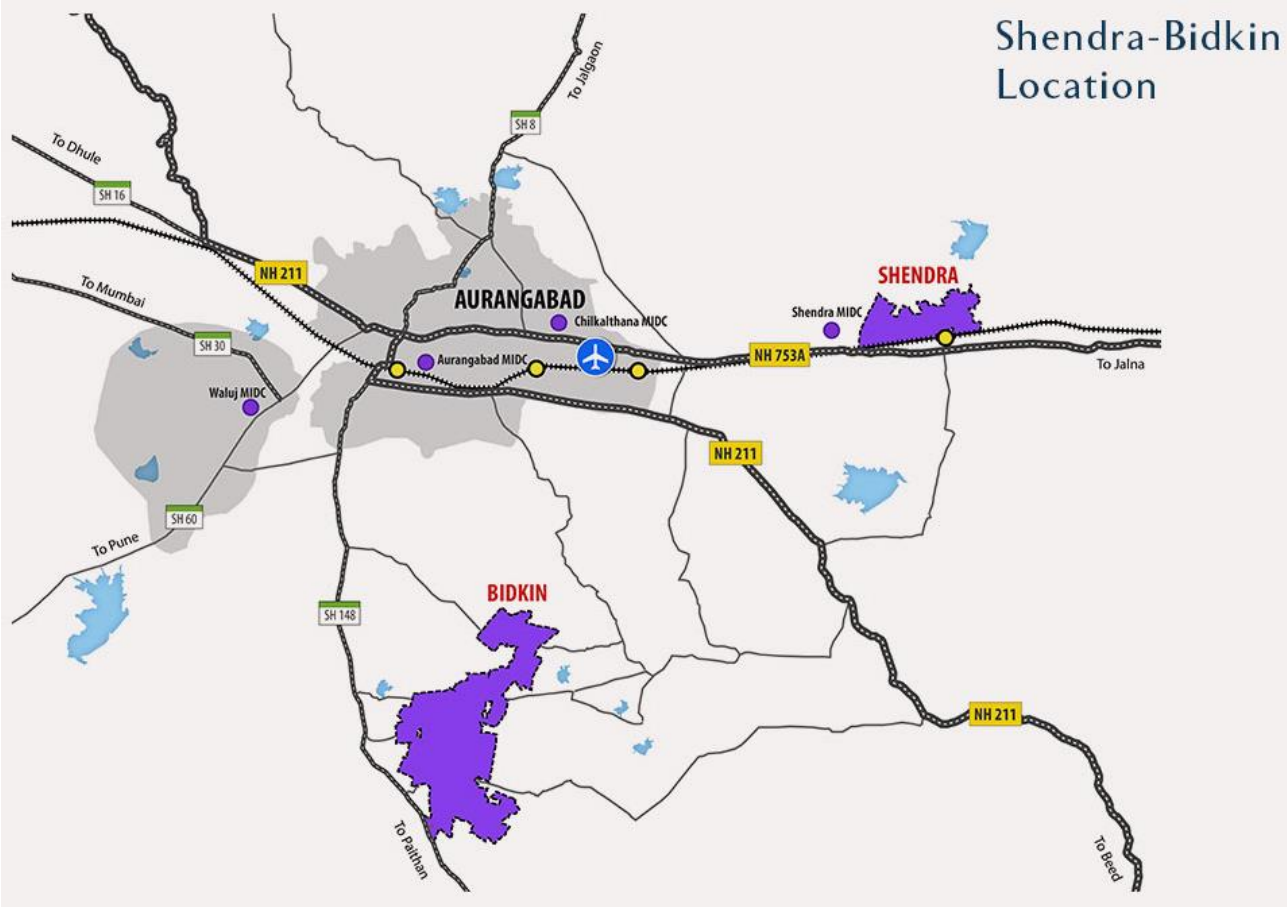


Exhibit 2: Shendra-Bidkin

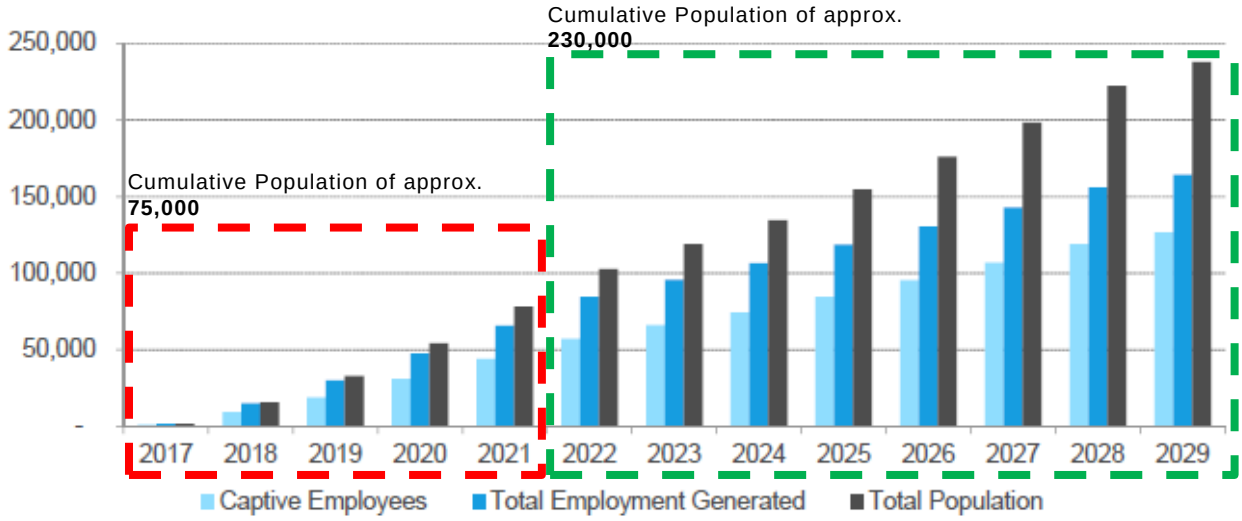


Exhibit 3: SBIA-Population Projection

Source: Techno-Economic Validation for Shendra-Bidkin Mega Industrial Park

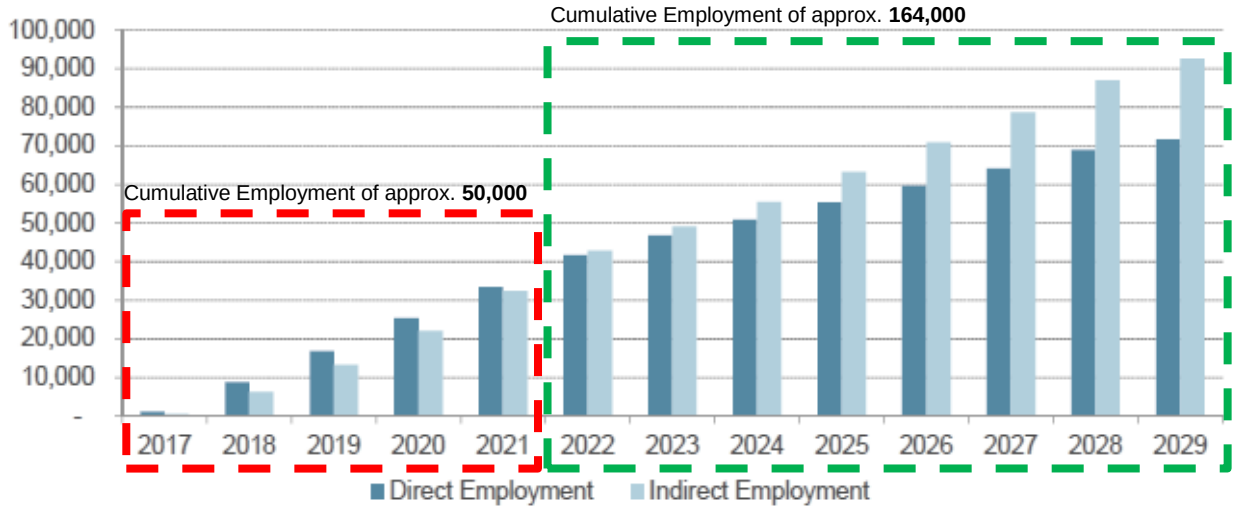


Exhibit 4: SBIA-Employment Projection

Source: Techno-Economic Validation for Shendra-Bidkin Mega Industrial Park

2 Project Overview and Components

AITL intends to implement a greenfield industrial smart city called AURIC. As one of the key initiatives for realizing this vision, AITL plans to implement a state-of-the-art ICT infrastructure along with various components for Bidkin area of AURIC as part of this Project. At the centre of the Project is the AURIC Control Centre (ACC), present in Shendra, which will be the nerve centre for the city. This ACC will be common for both Shendra and Bidkin areas of AURIC. A temporary and back-up control centre called Mini Control Centre (MCC) will be implemented in Bidkin which shall be integrated with ACC. All applications and sensors installed as part of AURIC will be integrated at the ACC and will be monitored/controlled from this common location. The ACC will interface with all end-devices and applications including at field level and at the user level. It will be the location from where the city will be operated and managed in terms of the infrastructure, critical systems and operations. All components that will be integrated at the MCC will communicate to the ACC using either wired or wireless communications. All Bidkin specific components will also be integrated with MCC from where, the feed will go to ACC in Shendra for centralized monitoring and control. The wired communications i.e. for the field devices and sensors will be over a purposeful-built fibre optic based infrastructure which will be deployed throughout the Project area. The fibre optic infrastructure will be used to meet both AITL needs and non-AITL needs i.e. tenants of AITL. It is desired that with this Project, an overall Fibre-to-the-X (FTTX) architecture is implemented for all field device connectivity and for connectivity to every plot. The wireless communications on the other hand will include purposeful built wireless network such as M2M communications for some field applications like utilities or will be realized using the city Wi-Fi network. The city Wi-Fi network will be deployed throughout the public areas of Bidkin and will be used to enable broadband to be accessible, affordable and available for the citizens. For applications such as e-governance, the citizen will use either the city Wi-Fi service or AITL's multi-services digital kiosks, or may use the respective connectivity from the respective Internet service provider.

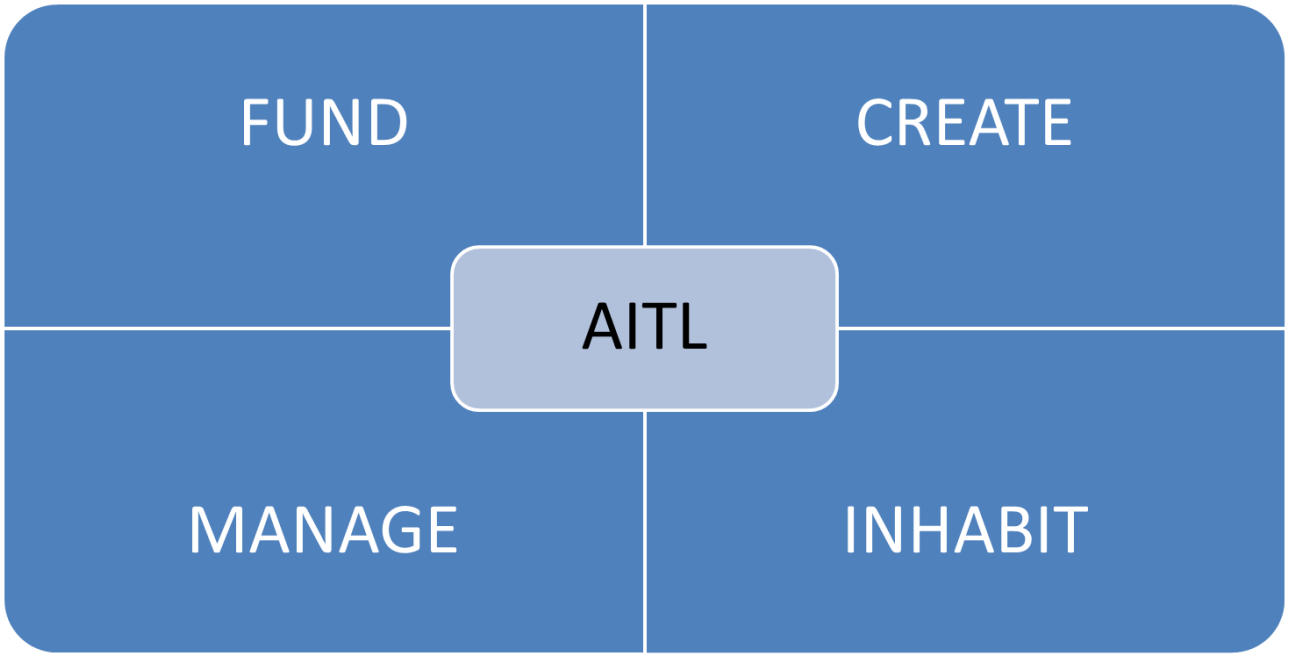
A smart city also includes the concept of safe city. AITL also plans to implement proactive CCTV surveillance system that will be used to monitor the city and its assets. In addition, automatic traffic counters and classifiers will be implemented at all entry and exit points of Bidkin Phase-1 to monitor traffic flows and other parameters. Automatic Number Plate Recognition (ANPR) cameras will also be implemented to monitor the number plates of vehicles travelling inside Bidkin in order to notify relevant authorities in case a hot-listed vehicle travels through the city premises. Environmental sensors will also be implemented at strategic locations for monitoring various parameters such as pollutant levels which will enable AITL to continuously track the environmental impact of the city.

As part of the AURIC smart city, it is also envisioned to develop and implement a Chatbot for AURIC services which act as an Inventor Management System with automatic replies to queries posed by Investors, Citizens and Businesses and also enabling automatic mail reminders to investors for required follow-ups.

Multiple e-governance services are being implemented for AURIC as part of AURIC-Shendra MSI project and AITL aims to provide 100% of citizen services online. The backend of the e-governance system and the backbone for AITL operations will be an Enterprise Resource Planning (ERP) system that will be primarily used by AITL for operating and managing the city. ERP system and e-Governance will be the one common system for Shendra and Bidkin and will be used by AITL for all activities required as part of the operations and management of AURIC. Bidkin MSI shall work in coordination with the Shendra MSI to integrate and develop all necessary functionalities which are required as part of Bidkin e-Governance and ERP.

AITL as an organization is expected to be lean. In addition, there may be outsourced services being managed by a City Manager who may operate some of the functions on behalf of AITL.

Being a greenfield site, AITL will need to go through the business cycle of Funding, Creating, Inhabiting and Managing the city as depicted in the below diagram. Note that part of this cycle is already underway and the details are only provided to help in providing background understanding of the Project.



Fund: The initial priority is funding the city infrastructure from various internal and external sources based on investment plans, which in turn are based on various projects and their funding needs. FUND function will also need facility to manage various sources of funds and their utilization on various projects. The internal sources of funds will be mainly from allocation of land. However internal sources of funds will become active only after land allocation starts. In addition, there could be various projects that could be taken in Public-Private-Partnership (PPP) mode. These projects will be jointly funded and as such will need to be monitored from that aspect. A time scale plan of investment and sources of funds will need to be created to manage the funds and their utilization. The key functions of funding the city are:

- Budget and Grant Management;
- Allocation of Land and Revenue Management;
- Public Private Partnership Management;
- Investment Planning.

Create: Once the city is funded, various planned projects need to be executed. This function is broadly termed as “Creating” the city. The manner in which the creation of city is conceptualized and executed will determine the pace of progress in attracting industrialists/entrepreneurs to invest in the city. The projects need to be executed in a manner that AURIC is created as a world class industrial city meeting the broad objectives of AITL.

Main use of funds in creating the city will be in land development, infrastructure creation like network, water, electricity facilities, and other city infrastructure, civic facilities like parks, clubs, social infrastructure, street lights etc. The city needs to be created in a manner that industrialist and citizens alike choose it over other investment and residential options. The key elements of creating the city are:

- Build Infrastructure for city development:
  - Telecom and other ICT infrastructure;
  - Power;
  - Water;
  - Water Treatment;
  - Waste Management;
  - Land Allocation and Road infrastructure;

  - Progress tracking for all the above projects.
- Land allocation for Commercial, Education, Residential establishment;
- Create Social Infrastructure like Parks, Clubs, Healthcare, Education, Library etc.

The key business objective for AITL in this phase are:

- Manage the grants and funds allocated by the stakeholders;
- Control the budgets and monitor the projects for building the trunk infrastructure;
- Generate funds by attracting private partners and businesses to invest in land and facilities.

Inhabit: Once basic infrastructure is in place and plans are afoot to create the city, efforts need to be started for attracting and retaining industrialists and citizens to the city. Facilitation centre needs to be created to answer queries of prospects. In parallel, tie up with various private and government agencies are required to be done to cover all the functions required to run the city. All civic amenities need to be in place and in working condition. A showcase to the current state and progress chart is required to be made available to all prospects. AITL is also vested with municipal powers and availability of municipal functions will be key in attracting citizens. Various functions in making the city inhabitable are:

- Attract and retain entrepreneurs;
- Provide unique ID to entrepreneurs and citizens;
- Facilitate Citizens and Residents;
- Provision of digital locker for citizens and entrepreneurs to store their documents;
- Enable Commercial/ Social/ Health facilities;
- Provision of services like Fire, Police, Traffic;
- Operate city and its Infrastructure;
- Provide Civic amenities and utilities;
- Provide Municipal Functions under purview of AITL.

Manage: Even before first citizens and industrialists inhabit the city, robust practices of managing the city needs to be provisioned. Inhabitants, citizens and industrialists alike will be able to request for any service through multiple channels like kiosks at suitable places, telephone, walk in to customer centre, mails or through interactive mobile application. The centralized city command and control centre will have the tracking feature to know issues proactively in any segment of city infrastructure. City Manager will have service level agreements to ensure level of service to be provided to inhabitants. Once city is operational, there will be provision required to carry out minor works encompassing electrical, telecom, water, waste water, roads, parks, streetlights, social infrastructure of the city. SCADA based systems and alarms will be used to proactively monitor water and electricity distribution network among other utilities. Citizen engaging services will be channelized through the use of city Wi-Fi infrastructure. Various functions under managing the city are as under:

- Monitor key performance indicators;
- Operate and Manage Infrastructure Services through City Manager;
- Command and Contact Centre Driven services delivery mechanism;
- Self-service Kiosks for enhanced user experience;
- Service Level Management;
- Escalation Management with vendors;
- Minor works Management;
- Revenue and Expense Management;
- Billing for services such as water, power and telecom as applicable.

Key Stakeholders in the System

The key stakeholders that shall be the direct/indirect users of the system are:

- AITL employees;
- Citizens residing in the city as well as industrial workforce;
- Any outsourced employees, managing the various city functions as applicable;
- Third Party Vendors;
- Other Government Departments/Organizations;
- Industrialists

A summary of the Project components that shall be implemented by the MSI as part of this Project are presented below:

COMPONENT	PROJECT REQUIREMENT
Fibre Optic Infrastructure	End-to-end fibre optic infrastructure (passive and active) to meet all the current and future needs of the Project with an overall architecture of Fibre-to-the-X (FTTX) for a connected city using various Points-of-Presence (PoP) facilities.
Public Wi-Fi	Public Wi-Fi to make broadband services more accessible, affordable and available for citizens and workforce across Bidkin Phase-1.
CCTV Surveillance System including Automatic Traffic Counter and Classifier (ATCC) and Automatic Number Plate Recognition (ANPR)	• CCTV surveillance system for proactive monitoring of strategic areas and infrastructure across. • Automatic Traffic Counters and Classifiers (ATCC) for monitoring flow and type of traffic at all entry/exit points of Bidkin Phase-1. • Automatic Number Plate Recognition (ANPR) cameras to monitor the number plates of vehicles travelling inside Bidkin Phase-1.
Multi-Services Digital Kiosk	Integrated and interactive multi-services digital kiosks for citizen services and emergency communications with Wi-Fi and CCTV across various public areas.
Environmental Sensor	Implementation of environmental sensors at strategic locations in Bidkin Phase-1 for monitoring of various parameters such as temperature, humidity, wind speed, rainfall and pollutants.
Solar Panel with Batteries	Solar panel with integrated battery at poles where ICT infrastructure will be mounted.
IT and other common Infrastructure	This includes implementation of complete IT Infrastructure to be provided as part of this Project such as Operator Workstations, Communication Cabinets with Racks, Servers, UPS, Data Security Solutions and Databases etc.
Streetlight Control System	To monitor and control the status of streetlight infrastructure at a grouping level and integrate with existing system.
Chatbot Solution for Investor Management	Digital interface to automate overall investor management processes and citizen / business interactions.
AURIC-Bidkin Mini Control Centre (MCC)	Mini Control Centre (MCC) which will act as the backup and temporary command and control centre for Bidkin. MCC will be fully integrated with AURIC Control Centre (ACC) in Shendra for centralised monitoring of AURIC.
Integration with AURIC e-Governance and ERP (AEE) and other services	This includes development, customization and integration of all necessary functionalities required for integration with AEE and other smart city applications.
Telecom Connectivity between Shendra and Bidkin Phase-1	Dedicated telecom connectivity to integrate the city operations of AURIC-Bidkin Phase-1 with AURIC-Shendra.

Overall, the expectation from this Project is that:

- The solution architecture should be open, interoperable and scalable;
- Adherence to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development);
- The overall architecture shall support:
  - Expandability: Open ended; allows upgrading to take advantage of continued evolution in transportation information and control systems;
  - Interoperability: Machine independent; allows the largest-possible markets for deployment;
  - Compatibility: Non-interference; various devices within the same system must be able to operate without interfering with the operation of other devices;
  - Interchangeability: Vendor independent; devices from different vendors that perform the same functions may be interchanged;
  - Open: Non-proprietary; promotes rapid development of new technologies and acceptance by consumers;
  - Scalable: Flexible; standards recognize local conditions with a wide range of ICT devices and communication channel capabilities. Legacy systems are accommodated to the extent possible;
  - State-of-the-art: Use of the best available standards to avoid locking in obsolescent technologies.
- Minimize the infrastructure such as poles, by co-locating various equipment (CCTV, Wi-Fi, Sensors, switches etc.) on streetlight poles.

Along with the implementation of the above mentioned components by the MSI, the MSI shall also be responsible for end-to-end coordination and integration with the following components (provided by Others). This has been further expanded in the detailed scope of work section of this RFQ cum RFP.

COMPONENT	PROJECT REQUIREMENT
Triple Play Voice, Video and Data Services	AITL plans to lease out dedicated backbone and distribution fibre optic infrastructure to the Telecom Service Providers (TSPs) as part of this Project. This fibre optic infrastructure will be implemented by the MSI and will be used by the TSPs. AITL will essentially provide 'dark fibre' to the TSPs and will provide TSPs dedicated space for co-locating their respective equipment at PoP rooms. MSI shall coordinate with various TSPs to incorporate their requirements in terms of dark fibre infrastructure.
Passive Infrastructure for Cellular Services	A tower company will be appointed by AITL for the installation, operations and maintenance of passive infrastructure for cellular services including cell phone towers and integrated smart poles. AITL will also provide dedicated space to the tower company for installation of towers and co-location of equipment (provided by cellular service providers). The MSI shall coordinate with the tower company and incorporate their requirements in terms of passive infrastructure.
ICT interface with Power, Water and Street Lighting Infrastructure for Internet of Things (IoT)	At present, EPC Contractor is implementing the civil and utilities trunk infrastructure. The water, power and street lighting infrastructure being provided by the EPC Contractor will be SCADA based and will be integrated at the MCC and ACC for the purposes of monitoring and control of critical parameters. The integration of these SCADA enabled utilities at the MCC and ACC and complete coordination with the EPC Contractor shall be the responsibility of this MSI.
Hosting Services	AITL has appointed a cloud service provider for meeting the hosting needs of the Project. Part of the Project IT infrastructure in the form of servers will be used via Infrastructure-as-a-Services (IaaS) provided by the cloud service provider. This will be used by the MSI for hosting services and infrastructure as detailed in this RFQ cum RFP.

COMPONENT	PROJECT REQUIREMENT
Civil Trench for Fibre Optic Infrastructure	EPC Contractor shall be providing the civil trench for the fibre optic infrastructure at majority of the places for backbone and distribution network. Details of this trench have been provided as part of this RFQ cum RFP. The MSI shall use this civil trench for the fibre optic infrastructure and coordinate with the EPC Contractor as needed.
e-Land Management System	AITL has implemented an e-Land Management System (e-LMS) which is being used for land allotment and management. The MSI shall be responsible for complete integration with this e-Land Management System.
AURIC-Shendra Existing Applications	Implementation of ICT infrastructure is currently underway at AURIC-Shendra. Bidkin Phase-1 MSI will be required to directly coordinate with Shendra MSI for integration with AURIC Control Centre (ACC), Video Management System (VMS), AURIC e-Governance and ERP (AEE) and various other smart city services and applications.

2.1 Project Phasing

The Project and its components shall be implemented in a phased manner which will broadly be in-line with both the Client requirements and the availability of on-site civil infrastructure. Note that since the EPC Contractor is responsible for the civil and utilities trunk infrastructure and the MSI is responsible for the Mini Control Centre (MCC) construction, the overall implementation of the Project is dependent on both these agencies which has been captured in the proposed phasing. If the respective on-site civil infrastructure is ready before time, the MSI's Project plan shall be flexible to accommodate the implementation of these modules before time. Some Project components may be implemented in parallel under different phases. The quantities of implementation as mentioned in table below will be finalized on the basis of Detailed Project Report (DPR) to be submitted by MSI as part of its first deliverable.

Note that the Bidder shall refer to all the sections of the RFQ cum RFP and the Bill of Quantities (BoQ) for exact quantities and requirements for implementation of the Project components.

TIMELINES	PROJECT MILESTONES/DELIVERABLES
T+2 Months	Project Study Phase – Detailed Project Report (DPR)
T+6 Months	Phase 1 – 30% implementation of BoQ (major line items)
T+8 Months	Phase 2 – 50% implementation of BoQ (major line items)
T+10 Months	Phase 3 – 70% implementation of BoQ (major line items)
T+12 Months	Phase 4 – • 100% implementation of BoQ; • Completion of burn-in period and operational acceptance of the Project; • Commencement of comprehensive maintenance phase.
T + 84 Months	Comprehensive Maintenance Phase

2.2 Business, Functional and Technical Requirements

2.2.1 Fibre Optic Infrastructure

2.2.1.1 Overview

An underlying enabler of a smart city is a highly reliable and available fibre optic infrastructure. AURIC will be the one of the first city of its kind that will have an end-to-end fibre optic infrastructure with an overall FTT-X architecture for all its services. This infrastructure will be used for both AITL and non-AITL services including AITL tenants. It is expected that overall, fibre optic infrastructure will be used for connectivity to all 'things' being implemented as part of AURIC-Bidkin Phase-1 area and will be the underlying enabler for connectivity.

The end-to-end fibre optic infrastructure shall be provided as per the following:

- A total of three (3) PoP facilities shall be provided for co-location of equipment and fibre optic termination for both AITL and non-AITL (including TSP) needs;
- Among these three (3) PoP facilities, a dedicated fibre optic infrastructure shall be provided in a ring architecture. This fibre optic infrastructure shall be dedicated for backbone communications of the Project;
- From each of these PoP facilities, there will be a dedicated fibre optic infrastructure required for distribution communications of the Project. This distribution communications will be used to provide connectivity to AITL field devices and for connectivity to plots in a dual homed based ring configuration;
- The last layer for communications will be the access layer i.e. connectivity to every plot and field device that will be provided from the distribution network. This is further divided into two (2) scenarios:
  - For AITL plots – access communications includes connectivity from the distribution communications trench until the Main Telecom Room (MTR) of the building. This includes fibre optic civil infrastructure and network cabling;
  - For non-AITL plots – access communications also includes connectivity from the distribution communications trench until the MTR of the building. However, in this case, the MSI will only provide fibre optic civil infrastructure (ducts) from the nearest manhole just until outside the property line of the respective plot;
  - For field device – access communications to all AITL field devices.

The AITL network is envisaged to have the following key attributes:

- Reliability, Availability and Resiliency: AITL network for AURIC shall have a high degree of reliability, availability and resiliency, even in the event of failed links, equipment failure, and overloaded conditions with a self-healing architecture. In addition, the failure of a single link or piece of equipment should not impact the overall network performance;
- Scalability: The network shall be scalable that can grow to include new user groups and can support new applications without impacting the level of service delivered to existing users;
- Manageability and Sustainability: Once designed and developed, the AITL available network staff must be able to manage and support the network. In order that it functions effectively and efficiently;
- Affordable and accessible: The services utilizing the AITL network (TSP) will be affordable and within reach of the target consumers;
- Publically Available: AITL network shall be publically available to encourage Internet penetration and GoI's initiatives like Digital India;
- Generate Revenue: AITL network of AURIC shall be able to generate revenue for AITL so that it is sustainable and profitable.

2.2.1.2 Architecture

Backbone Architecture

The backbone will be designed between Primary Point of Presence (PoP) and other two (2) secondary PoPs. Primary PoP will also accommodate Mini Control Centre (MCC) for AURIC-Bidkin. There will be a requirement to connect AURIC Control Centre (ACC) located at AURIC Hall Building in AURIC-Shendra to the Mini Control Centre (MCC) at the Primary PoP location at AURIC-Bidkin Phase-1 area.

Proposed backbone network connectivity between each Point of Presence has been shown in Exhibit 5 below. The backbone architecture for AURIC-Bidkin Phase-1 is being proposed as ring where all of the data that is transmitted between the PoPs will take the shortest path (or least costly path) between PoPs with high reliability, resilience and survivability. In the case of a failure or break in one of the links, the data shall take an alternative path to the destination. Each PoP shall be connected to the two (2) other PoPs for high availability, reliability and survivability of the overall backbone fibre optic network. Currently, there is no direct connectivity between Shendra and Bidkin areas of AURIC, and a temporary backbone connectivity using telecom links will be required until a permanent connectivity via future fibre infrastructure comes in place.

The overall backbone network connectivity shall be designed and developed in a manner that each link shall be able to meet its individual zone requirement while accounting for redundant network switching capacity required in case of any link failure along with provision for future growth in terms of bandwidth requirements of the network. The backbone network shall be continuous, i.e. there shall be no field splicing of the backbone network and all terminations of the backbone network shall happen only at the PoP facilities.

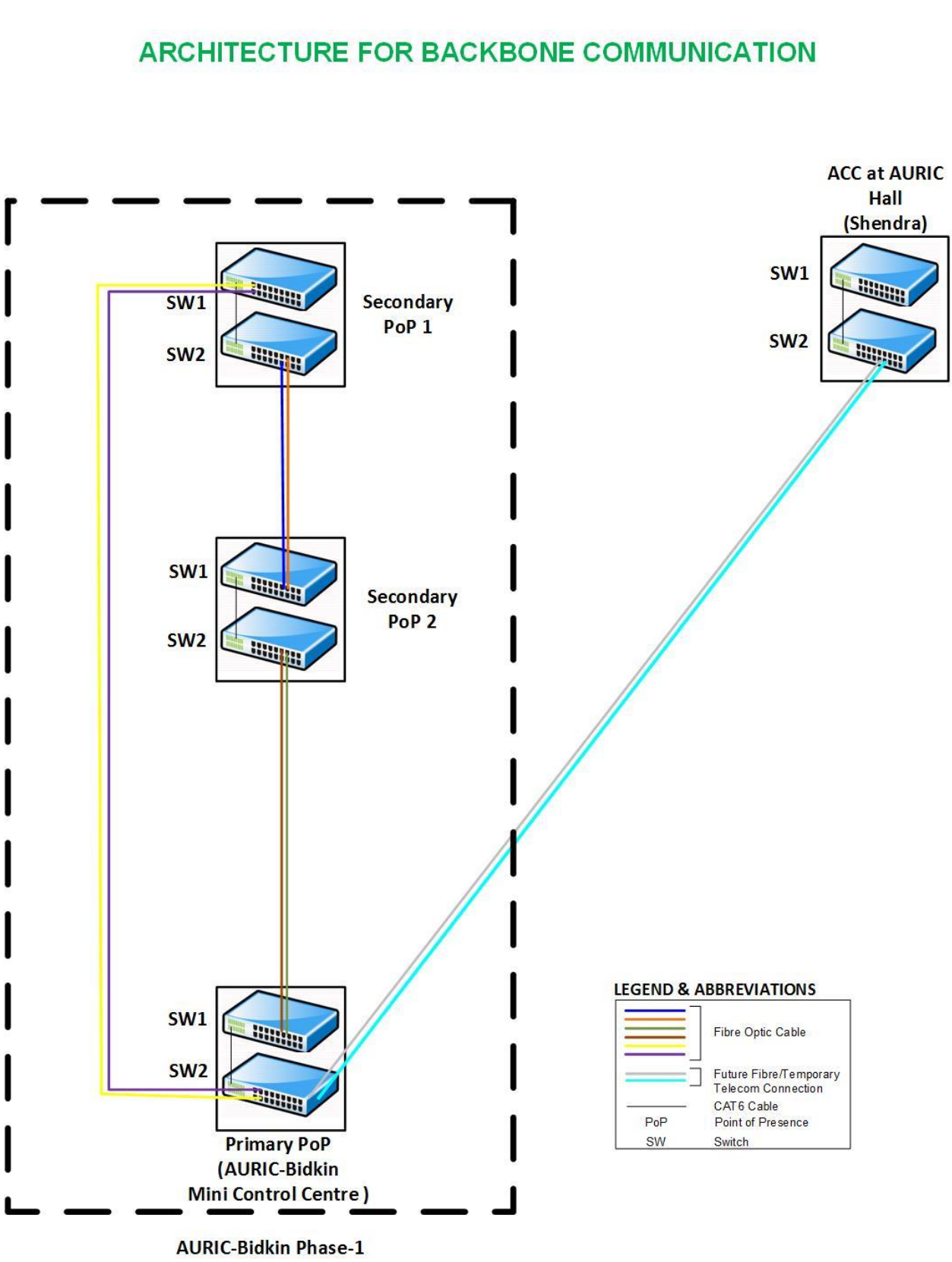


Exhibit 5: Indicative Architecture for Backbone Communications for AURIC-Bidkin Phase-1

Distribution Architecture

The distribution architecture shall be Layer 2 based which shall be designed for a ring configuration for the fibre optic network. This ring shall be created using redundant PoPs and geographically redundant paths wherever available. The distribution fibre shall further be used to connect a particular 'zone' from a respective PoP location. This zone shall include distribution connectivity to both plots and end-devices.

Access Distribution for City-wide AITL Services

Using the distribution network, the access network shall provide end-to-end connectivity to the field devices and plots. The access network will be divided into the following parts:

- For AITL field devices;
- For AITL plots;
- For non-AITL plots.

Active Electronics for Fibre Optic Network

All the network switches at access level (field) shall be Layer 2 based and shall be industrial grade, suited to perform as per on-site conditions.

All the network switches at distribution level (PoP) shall also be Layer 2 based but may not be industrial grade. Further, all network switches for backbone (PoP) shall be Layer 3 based.

Point of Presence

Point-of-Presence (PoP) rooms are where all city services (AITL and non-AITL) shall originate/terminate. This space will be shared between AITL services and tenants including Telecom Service Providers (TSPs) and cellular among others. There will be one (1) primary PoP and two (2) secondary PoPs proposed at geographically distributed locations across AURIC-Bidkin Phase-1. The PoPs shall have dedicated space for each of the tenant and AITL services. They will also have the main cellular towers co-located in the same plot location with dedicated space for cellular services.

The PoPs shall be categorized and sized as follows:

- One (1) Primary PoP (which shall accommodate MCC as well): Total approximate area of 4000 sq. ft. including approximately 1000 sq. ft. for MCC;
- Two (2) Secondary PoPs: Approximate area of 1,400 sq.ft.

Note that it is expected that the PoP will not just cater to AURIC-Bidkin Phase-1's needs today but also future growth in terms of space requirements and support tenant co-locations. Based on the building size of PoP facility and tower, a setback in compliance with the development guidelines will be required for sizing the entire plot area.

Telecom Services

Various telecom services including voice, video, data and cellular will be provided as part of AURIC-Bidkin Phase-1. The voice, video and data services for every plot will be provided by respective telecom service providers using the AITL fibre optic infrastructure at AURIC-Bidkin Phase-1. Each TSP shall get a dedicated 48 count fibre optic backbone throughout Bidkin Phase-1. This 48 count backbone shall be installed inside dedicated conduit infrastructure and will be provided between all PoP locations and end-to-end across Bidkin Phase-1. Further, based on the detailed design, there will be dedicated duct between manhole and plot for TSPs where required. The TSPs will be provided dedicated space inside each PoP for their respective actives, passives and services. For all plots except selected AITL plots, the conduit infrastructure will be terminated just outside the property line. For AITL plots, the conduits will be terminated close to the Main Telecom Room (MTR). However, all other actives and passives required for plot connectivity shall be provided by respective TSPs.

For cellular services, AITL shall provide space inside the PoP rooms. However, there will be a tower company (direct or via ICT MSI) appointed for providing all infrastructure associated with cellular services including towers, cabling, antennas etc. AITL will provide the land as part of the PoP room for installing these towers. All the PoP rooms will have a cellular tower installed as there are no nearby existing cellular towers in AURIC-Bidkin Phase-1.

BR - 1 Business Requirements

BR 1.1	End-to-end city wide fibre connectivity is required as a part of the project to support the smart city functions and enhance the quality of services for the citizens.
BR 1.2	AITL shall own all end-to end fibre infrastructure including trench, cable tray, duct, fibre, splices, and other accessories and will become a dark fibre provider for all AITL right of way.
BR 1.3	The fibre optic infrastructure shall be utilized by AITL as well as other city agencies (upon approval of AITL) as a common ICT infrastructure.
BR 1.4	Overall network shall be divided into three (3) parts: backbone, distribution and access networks. AITL to provide end-to-end backbone and distribution networks for all purposes along with access network for field devices. For access networks to plot, depending on the plot type, it will be a combination of AITL and respective plot developer that will provide this network.
BR 1.5	There will be three (3) Point of Presence (PoP) rooms that will be the co-location and aggregation facilities for an integrated high-speed network backbone. The PoP rooms will be the co-location spaces for both AITL network and non-AITL network (leased to various tenants). Each of these PoPs shall be connected over a dedicated high speed backbone network that will support a carrier grade, IP/MPLS based ring architecture. Each of the PoPs will provide dedicated connectivity using the distribution layer and serve a particular 'zone'. A 'zone' has a group of devices and plots that will ultimately be connected using the distribution and access network. Connecting the distribution layer, there will be the access layer i.e. the access network that will provide connectivity to the respective end-devices and plots.
BR 1.6	Manholes and handholes/pits shall be placed at strategic locations for the fibre optic infrastructure throughout the AITL RoW. These manholes shall be used for placing the Fibre Optic Splice Enclosure (FOSC) while the handholes/pits shall be used for pulling of fibre if required. Placement of these manholes and handholes/pits will be under MSI's scope of work.
BR 1.7	Manholes shall be provided at every splice location which shall cater to current and future splice requirements.
BR 1.8	AITL shall provide Point of Presence (PoP) rooms to the TSPs and other tenants and lease out space to them.
BR 1.9	For the TSPs, cellular and other tenants, only the 'bare-shell' infrastructure (including at least one light point and room DB) with partitioned space within the PoP shall be provided as a part of this Project. The tenants shall be responsible for using this 'bare-shell' infrastructure space and provide all their required actives inside their dedicated space.
BR 1.10	The overall network architecture shall support a ring for backbone and distribution communication network. Maximum number of rings per pair of fibre shall depend on the detail design. All rings shall be dual home based architecture.
BR 1.11	AITL network shall be reliable, interoperable, open standards based, available and resilient. It shall be scalable, manageable, supporting segregation of traffic and sustainable. It shall also generate revenue for AITL.
BR 1.12	All backbone networking shall be IP/MPLS based.
BR 1.13	All backbone electronics shall be sized with sufficient capacity to support the redundancy and future traffic growth in order to complete traffic rerouting on the backbone in event of a fibre or switch failure without impacting overall network performance.
BR 1.14	For distribution architecture, all AITL plots will have redundant entry and exit fibre paths for connectivity until the plot levels with redundant FOSCs and single switch at the telecom room of the building.
BR 1.15	For distribution architecture, all non-AITL plots will have single entry and exit fibre path for connectivity until the plot level with single FOSC outside the plot.

BR 1.16	As AURIC is being developed as one of the first greenfield industrial smart cities, high priority is placed on the city's ICT infrastructure to be a key enabler in providing modern triple play services to the citizens. As part of the ICT infrastructure, AITL will provide the entire passive infrastructure i.e. dark fibre infrastructure for TSPs and other tenants for both backbone and distribution network.
BR 1.17	All splicing for distribution network of TSPs and other tenants shall be the responsibility of the respective TSPs and tenants under the supervision of AITL.
BR 1.18	AITL is registered with DoT as Infrastructure Provider Category I (IPI) to establish and maintain the assets such as Dark Fibres, Right of Way, Duct Space and Tower for the purpose to grant on lease/rent/sale basis.

FR - 1 Functional Requirements

FIBRE OPTIC CIVIL INFRASTRUCTURE- TRENCH/ DUCT/ MANHOLE	
FR 1.1	The backbone and distribution trench for 60m, 45m, 30m, 24m Right-of-Way (RoW) – In this case, there shall be a concrete encased trench that will be provided by the EPC Contractor along the road. The concrete encased trench shall be provided with a tray based system and shall have dedicated tray for fibre optic infrastructure for the duct installations.
FR 1.2	The backbone and distribution trench for 18m or less RoW – In this case, EPC contractor shall provide the HDPE ducts and manholes for fibre optic infrastructure at one side of road. MSI will use same ducts for backbone & distribution OFC networking. EPC Contractor will also provide the cross duct at all the junction crossings for crossing to connect the other side of the roads which will be used by the MSI for installing the fibre optic infrastructure.
FR 1.3	The access trench shall be provided by MSI for every plot and connectivity to every field device.
FR 1.4	The manholes (other than 18m) shall be provided by the MSI (including those required inside the AITL plots).
FR 1.5	The manholes shall be sized per approximately 1.2m x 1.2m x 1.0m (l x w x d) inside clear space.
FR 1.6	The fibre optic cable shall be installed inside dedicated Permanently Lubricated (PLB) High Density Polyethylene (HDPE) smooth wall configuration ducts inside the trench. These HDPE ducts shall be sized to provide sufficient future growth capacity for Bidkin Phase-1.
FR 1.7	HDPE duct shall be laid throughout Bidkin Phase-1 using both the concrete encased trench and open trench.
FR 1.8	The HDPE duct shall be suitable for underground fibre optic cable installation by blowing as well as conventional pulling.
FR 1.9	The HDPE duct shall be suitable for laying in RCC trench, trenches by directly burying, and laying through trenchless digging i.e. Horizontal Directional Drilling (HDD).
FR 1.10	There are following types of ducts for fibre optic laying to fulfill the end-to-end connectivity of the ICT infrastructure: • 8 times 1x40mm (OD) PLB HDPE ducts for backbone and distribution communications; • 1x50mm (OD) PLB (Orange colour) HDPE ducts for connectivity to every plot; and • 1x40mm (OD) PLB HDPE duct (Orange colour) to connect every field device location. ID for HDPE duct as per standard telecom industry practices can be provided.

FR 1.11	The tentative colour allocation for the backbone/distribution ducts are: • 2x40mm aqua colour, • 2x40mm orange, • 2x40mm blue and • 2x40mm slate.
FR 1.12	All HDPE ducts shall be colour coded as per EIA/TIA 598 standard.
FR 1.13	For access infrastructure to plots, there shall be two (2) scenarios: • For AITL plots, there will be dedicated connectivity required between the manhole and respective plot's Main Telecom Room (MTR). This connectivity will be provided using the 1x50mm HDPE duct configuration. • For non-AITL plots, the 1x50mm HDPE duct configuration will be provided until just outside the plot property line.
FR 1.14	For field device connectivity, each device shall have dedicated 1x40mm HDPE duct for access network.
FR 1.15	All the ducts shall be supplied with tracer wire and shall have in-built rodent protection chemical at outer sheath of every duct. Tracer wire is to be provided only in areas where there is open trench.
OPTICAL FIBRE CABLE (OFC) OR FIBRE OPTIC CABLE (FOC)	
FR 1.16	The AITL fibre optic network shall have an overall Fibre-to-the-X (FTTX) architecture.
FR 1.17	End-to-end fibre optic infrastructure shall include only single mode Optical Fibre Cable (OFC), loose tube, dielectric armoured cable configuration rated for outdoor & underground installations.
FR 1.18	All fibre optic cable shall be ordered in standard tube and colour configuration based on EIA/TIA 598.
FR 1.19	Each of the PoP rooms shall be connected over a dedicated 24 count fibre optic cable. This cable shall only be used for backbone communications and will not be field spliced. It will only be terminated at the PoP and will have redundant entry and exit paths to all PoPs for inside plot. This 24 count fibre optic cable shall be provided in two (2) separate tubes i.e. 12 count per tube.
FR 1.20	For distribution to plots, a dedicated 48 count fibre optic cable will be provided end-to-end in the respective zone. Similarly, for connectivity to AITL field devices, a dedicated 48 count fibre optic cable will be provided end-to-end in the respective zone. For AITL field equipment, it is expected that a lot of the field devices will be co-located i.e. leverage the same field infrastructure for mounting and use the same network switch. It is expected that the field devices like Wi-Fi and CCTV will share the same streetlight poles and will be connected over a ring architecture. All 48 count distribution fibre shall be ordered with fibre in four (4) tubes with 12 count per tube.
FR 1.21	For the TSPs and other tenants, a dedicated 48 count fibre optic cable shall be provided for each tenant. This will be provided with fibre in four (4) tubes i.e. 12 count per tube.
FR 1.22	For AITL plots, access network shall have dedicated 12 count fibre optic cable from the manhole to the respective MTR. This will be ordered with 4 count per tube configuration. For non-AITL plots, access network of fibre cable including FOSC and cable shall be provided either by the Telecom Service Providers or the Plot Holder between MTR of the plot and the AITL manhole. For AITL device connectivity, access network shall be provided via dedicated six (6) count fibre optic cable per network switch.
UTP COPPER CABLE AND ACCESSORIES	
FR 1.23	Outdoor-rated Unshielded Twisted Pair (UTP) Communications Category (CAT) 6 Cable to provide Ethernet connectivity between network switches and end devices such as CCTV, Wi-Fi, etc. located within 90 m from the switch location.

FR 1.24	The UTP cable shall be outdoor-rated UTP CAT 6 cable.
FR 1.25	Wherever installed, the UTP cables shall be supplied with either in-built surge suppressor or shall have additional surge suppressors as specified.
FR 1.26	Each conductor of the UTP cable shall be insulated with a coloured high density polyethylene jacket with varying twisted length to minimize crosstalk.
FR 1.27	Additional accessories to include CAT 6 Patch Cords required for data communications connections, CAT6 Patch Panels for cable termination and Surge Suppressors for protection from voltage spikes as per the design requirements.
FR 1.28	The UTP patch panels shall be sized to support the design requirements as per the RFQ cum RFP. At least 50% of the capacity of the patch panel ports shall be left as spare.
FR 1.29	The surge arrestor shall be such that they do not interfere with normal communications.
FR 1.30	The termination shall protect the cable terminations from water and mechanical damage and shall be resistant to salt corrosion.
FR 1.31	Any provided patch panel or wall plate shall provide mechanical support for all connections enclosed and shall maintain insulation between them.
FR 1.32	All cable entries shall be provided with appropriate cable pathway.
FIBRE OPTIC ACCESSORIES	
Optical Connectors	
FR 1.33	Optical connectors shall be used to terminate optical fibre for their interconnection and distribution.
Fibre Patch cords	
FR 1.34	Fibre Patch cords shall be used to connect Fibre Termination Panel to the network switch.
Fibre Distribution Management System (FDMS)/Optical Cable Entrance Facility (OCEF) and Fibre Termination Panels	
FR 1.35	OCEF/FDMS shall be installed at the PoPs and shall be used to manage all fibre entry/exit inside all PoPs.
FR 1.36	The OCEF/FDMS shall be equipped with splice trays to accommodate the requirement of this Project.
FR 1.37	The OCEF/FDMS shall have built in slots to secure fibre and management clips to hold spools of slack fibre.
FR 1.38	The OCEF/FDMS shall have identification labels inside the door.
Fibre Optic Patch Panel	
FR 1.39	Fibre Optic Patch Panels shall be installed at termination location at PoP, AITL plots and at every field switch location installed on the pole or cabinet.
FR 1.40	The Patch panels shall be capable of supporting SC/ST/LC type ports for backbone, distribution and access network.
FR 1.41	The Patch panels shall have the capacity for terminating the number of fibre as required per the requirements of the Project plus additional 20% spare for future.
Intelligent Patching System	
FR 1.42	At PoP rooms, intelligent patch panels shall be installed for AITL infrastructure.
FR 1.43	The Intelligent patching system shall comprise of intelligent patch panel, modules, and associated software to be provided at the PoPs locations to manage network planning, implementation and operational activities like moves, adds and changes.

FR 1.44	System Hardware shall be capable of seamlessly feeding information directly into the software platform.
FR 1.45	The software platform shall provide fully accurate and comprehensive documentation of all network infrastructure components as well as advanced detection and alert capabilities to allow full control over the environment.
FIBRE ASSET MANAGEMENT	
FR 1.46	With implementation of a fibre optic network, there is a requirement to create a fibre asset management system for management of the infrastructure.
FR 1.47	The fibre asset management system shall be a purposeful-built tool that will allow mapping of all fibre counts in terms of count colour, number and allocation (entity or device) among other variables.
FR 1.48	Fibre asset management system shall be configurable and easy to operate and update. It is expected that post any implementation of the fibre optic infrastructure, this asset management system shall be updated on an on-going basis.
ACTIVE ELECTRONICS (SWITCHES, MEDIA CONVERTERS, WIRELESS GATEWAYS)	
FR 1.49	Industrial grade, POE/POE+ enabled, Layer-2 Ethernet switches shall be installed at the field for connectivity to field devices.
FR 1.50	Non-industrial grade, Layer-2 Ethernet switches shall be installed per PoP for distribution to field devices and plots.
FR 1.51	Layer 3 based Ethernet Switch/Router shall be installed at all the Point of Presence (PoP) locations for communication between the PoPs.
FR 1.52	Core router for connectivity to the outside world i.e. for worldwide web services and for connectivity to the cloud service provider.
FR 1.53	Layer 2 switches at the field shall have minimum 1 Gbps backhaul fibre support.
FR 1.54	Each of the Layer 2 switches at the PoP shall support at least 1 Gbps per port (fibre) for distribution with backhaul uplink of 10 Gbps copper/SFP+ while the Layer 3 switches/routers at the PoP and MCC shall have 10Gbps support per port. Any attenuators required as part of the overall solution shall be provided by the MSI. Note that all fibre optic SFPs shall be ordered to support minimum 10 km distance for distribution and combination of 10km and minimum 25 km or more for backbone depending on the distance requirements. This shall be validated by the MSI during the design stage.
FR 1.55	The overall architecture of the system is such that there will be a ring configuration between all PoPs i.e. for Layer 3 switches/router and between all Layer 2 switches at the PoP.
FR 1.56	The switches from any one vendor shall be interoperable with other brands.
FR 1.57	Communications Media Converter to be installed, if required, on a per device basis where the distance between the IP enabled device and the respective switch is greater than 90m.
FR 1.58	The Communications Media Converter shall enable fibre to copper and copper to fibre media conversion for IP enabled devices. MSI may also use an Ethernet extender as an alternative to the Media converter based on prior permission from AITL.
FR 1.59	Wireless M2M Gateways to enable Internet of Things (IoT) shall be installed at cellular towers and/or streetlight poles if required.
FR 1.60	These gateways can support the data aggregation of the Smart Bins and for water and power meters (future).
FR 1.61	The gateways shall be capable of supporting continuous communications among all devices.
FR 1.62	All the active devices shall enable security features in the network switches to disallow any unauthorized access to the port / network.

NETWORK MANAGEMENT SYSTEM (NMS)	
FR 1.63	The NMS shall facilitate the retrieval, storage, analysis and display of status information from all network devices attached to the system that are SNMP and/or ICMP capable, and shall facilitate remote configuration of these devices.
FR 1.64	The NMS shall provide the ability to view the network and its associated IP SNMP/ICMP enabled devices including switches and other IP devices connected over the network. It shall support a minimum of 5000 end points.
FR 1.65	The NMS should include all hardware and software required to configure, control and monitor the network connected SNMP/ICMP based devices.
POINT OF PRESENCE (PoP)	
FR 1.66	PoP facilities are co-location spaces for both AITL and non-AITL infrastructure.
FR 1.67	Each PoP shall typically serve approximately 3 to 4 sq.km area.
FR 1.68	All PoPs shall be telecommunications grade facilities built for 24x7 operations. They should support a raised cable tray based design.
FR 1.69	Primary PoP (MCC) will serve as a primary hosting & backup control centre space for AITL for the support of all AITL applications that require local servers, video wall along with its controller and data storage (example CCTV) along with networking equipment and fibre terminations. It will also serve as the termination point for distribution fibre networks as well as nodes on the core backbone communications ring that supports intra-PoP communication. In addition, it will also be the telecom and cellular service providers' point of entrance to Bidkin Phase-1 and will house the respective service providers' equipment.
FR 1.70	Secondary PoPs will serve as the termination point for distribution fibre networks as well as nodes on the core backbone communications ring that supports intra-PoP communication. In addition, it will also serve as the telecom and cellular service providers' plus other tenant co-location facility and may also serve as their entry point to Bidkin. In addition, it will also be the telecom and cellular service providers' point of entrance to Bidkin phase-1 and will house the respective service providers' equipment.
FR 1.71	Each secondary PoP building shall have separate partitioned rooms for minimum 5 tenants including AITL.
FR 1.72	Separate access for AITL, TSP's and other tenants shall be required in the building. Bare shell infrastructure with partitioned space will be provided to all tenants within the PoPs.
FR 1.73	Each PoP area shall have Security surveillance using fixed CCTV that record entry and exit to prevent unauthorized entry as well as access control functionality along with electronic door locks.
ENTERPRISE MANAGEMENT SYSTEM (EMS)	
FR 1.74	The EMS shall be able to support the proposed hardware and software components (IT and Non-IT) deployed over the tenure of the Contract. The EMS shall be capable of providing early warning signals to the Helpdesk Agents on the performance issues, and future infrastructure capacity augmentation. The EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring.
FR 1.75	EMS shall provide at a minimum the following functions: • Configuration Management • Fault Management • Incident, Problem and Change Management • Asset Management • Remote Control

	• SLA Management & Monitoring • Performance Management • Monitoring Backup and Management • Event Management • Server, Storage and other Infrastructure Management • Monitor network components of the LAN & WAN • Network Link Monitoring • Helpdesk Monitoring, Management and Reporting • Traffic Analysis.
RODENT REPELENT SYSTEM	
FR 1.76	The entry of rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However, the MSI shall conduct periodic pest control using chemical spray once in a quarter as a contingency measure to effectively fight pests.

TR - 1 Technical Requirements

HDPE DUCT	
TR 1.1	At a minimum the HDPE duct shall meet or exceed the applicable industry standards as listed below: • TEC specification as well as IS:4984- 1995 for HDPE duct (For hydraulic characteristic only) • ISO standards (ISO 9001, ISO 14000) • ASTM D1693, D790, D1712, D4565, D2240, D638, D648, F2160, G154 • IS 2530, 4984, 7328, 9938, 12235(Part-9), 14151(Part-1) • TEC specifications • Other standards as detailed in this specification
TR 1.2	The HDPE ducts shall be installed end-to-end across Bidkin. They will be used for backbone, distribution and access communications.
TR 1.3	The HDPE ducts shall be ordered in different configurations and colours as detailed in the functional requirements. These colours shall be maintained throughout the useful life of the duct.
TR 1.4	The 40 mm (OD) with 3.5mm+/-0.2 mm wall thickness and 50 mm (OD) with 4.0mm+/-0.6 mm wall thickness coilable HDPE ducts shall be of smooth configuration and shall be suitable for outdoor underground installations.
TR 1.5	All HDPE ducts shall be continuous. Where the duct reel ends, the HDPE ducts shall be joined using approved industry standard couplers or inside manholes/handholes/pits. Where couplers are used, they shall be single piece HDPE coupler which shall be used to provide water proof and air proof secure fit in accordance with the manufacturer's recommended procedure for joining ducts.
TR 1.6	The duct sweeps shall not exceed 180 degrees for the sum total of duct sweeps for a section of duct between duct termination points.
TR 1.7	The duct shall be free from visual defects like blisters, shrink holes, flaking, scratches groove lines & roughness.
TR 1.8	The duct shall have in-built rodent protection.
TR 1.9	Minimum Bending Diameter shall be at least 15 times of outer diameter (OD) of the duct or as per standard manufacturer recommendations.

TR 1.10	Bending Performance: There shall be no damage when mounted on a mandrel of duct diameter for 30 minutes.
TR 1.11	In the HDPE Duct, the coextruded inner layer of solid permanent lubricant shall be integral part with HDPE and white in colour, clearly visible in cross section of duct. The inner lubricant material shall be of friction reducing, polymeric material & should be min. 10% of wall thickness. The lubricant materials shall have no toxic or dermatic hazards for safe handling.
TR 1.12	The coil shall be at least 300 meters in length.
TR 1.13	The pre-installed PP rope/Fishline shall be ordered along with the PLB duct. In this case PP rope/Fish line is safely tied to the end caps at either ends with hooks to facilitate pulling of the OFC cables at a later stage. The rope shall be polypropylene, and shall meet IS: 5175 standard. It shall have 1.5m of line coiled in the bottom of manholes at the end of each duct run.
TR 1.14	The duct shall be supplied with atleast 0.6mm diameter in-built copper tracer wire. The tracer wire shall be 12 gauge, copper 600V insulated blue wire in all empty conduits. The tracer wire shall interconnect in the manholes. Tracer wire terminals shall have a tag to identify it as AITL fibre. This tracer wire shall be provided for all sections where there is open trenching.
TR 1.15	The HDPE ducts shall be supplied in reels or coils after sealing both ends by end caps. The following markings shall be provided on each packing: • Code of product • Name of Manufacturer • Date of manufacturing • Length of PLB HDPE duct • Dimension of Outer diameter and Inner diameter • Client's name.
TR 1.16	All the duct shall be clearly marked with indelible ink at intervals of 1 meters with the following data which is not less than 5 mm high. Neither the colour of the duct nor the marking printed inscribed on it shall change or fade away throughout the life time of the duct. The details of marking on duct shall be approved by AITL before commencement of manufacturing: • AITL with logo • Manufacture’s name or trade mark • Year and month of manufacturing • Type of PLB HDPE duct and size • Running length marking.
Laying of PLB HDPE Duct in Open Trench	
TR 1.17	HDPE ducts shall be laid in open trench for less than 24m RoW or for access to plots/devices.
TR 1.18	The duct trench shall be dug as per route plan (indicating the various dimensions and other details of the trench) approved by the AITL for each type of soil type.
TR 1.19	Due care and precaution during excavation shall be taken to avoid possible damage of any other underground plans/facilities in the proposed underground PLB HDPE Duct route and shall indemnify AITL for all damages and shall be solely responsible for all the damages and losses.
TR 1.20	The minimum depth at which the duct shall be laid will be in compliance with DOT norms and telecom best practices.
TR 1.21	No blasting is permitted near permanent work or dwellings. Blasting shall be so made that pits are as close to the designed dimensions as practicable.
TR 1.22	The width of trench at the top and bottom shall be adequate for proper installation of PLB HDPE ducts with required quantities.

TR 1.23	The trench depth shall be measured from the bottom of the trench. Trench shall be located at the lowest point of lower area, if possible.
TR 1.24	In case of uneven ground, the MSI ensure that the bottom of the trench is not uneven, the MSI shall maintain minimum depth of the trench as per specifications and may be required to increase the depth at some locations and provide a suitable gradient in the trench.
TR 1.25	The backfilling and compacting of trench in layers of 200 mm, restoration of road, nalla, pavements etc. after the completion of laying work.
TR 1.26	Provided that the PLB HDPE ducts has been properly laid and jointed in the trench, and the back filling operation shall follow as closely as practicable.
TR 1.27	The back filling operation shall be performed in such a manner as to provide firm support under and above the PLB HDPE duct and to avoid bend or deformation of the PLB HDPE duct, when the PLB HDPE duct gets loaded with the back filled earth.
TR 1.28	Where in any location the back filling is unevenly centred over the trench due to carelessness or any other cause, it shall be redressed at the MSI's expenses.
TR 1.29	No debris shall be allowed in backfill at any time.
TR 1.30	At locations where the backfill material contains hard rocks, rock fragments and other hard materials which may cause damage to the pipe and where rock has been excavated from the trench and it is intended to refill the trench, the trench shall be initially filled. De-rocked loose earth above the top of the duct shall be screened through a suitable mesh if so required and backfilling only thereafter be completed and finished with excavated material.
Laying of PLB HDPE Duct in RCC Trench	
TR 1.31	RCC Trench shall be provided by the EPC Contractor. MSI shall lay the HDPE duct for fibre inside this RCC Trench end-to-end.
TR 1.32	The HDPE duct inside RCC Trench shall be laid using a tray based system supported by brackets. This shall be applicable for all RoW excluding 18m or less. Any core cutting required to exit / enter this RCC trench for ICT requirements shall be provided by the MSI.
Other Installation Requirements	
TR 1.33	During transportation and storing at the site duct, it is necessary to seal the ends of the duct with proper End caps against water penetration or other impurities.
TR 1.34	When installing duct in an open trench from a drum, it should be uncoiled from the bottom and not from the top of the drum.
TR 1.35	The fill ratio of the duct shall be in compliance with the National Electric Code (NEC) standard NFPA 70, ANSI/TIA 568 and ANSI/TIA 569.
TR 1.36	When placing multiple ducts in a single trench simultaneously, it is important not to cross or twist the ducts inside the trench, when installing large quantities of ducts it is possible to stack them one on top of the other in addition to side by side.
TR 1.37	Positioning of the ducts must be designed in the planning stage to ensure clarity between ducts placement.
TR 1.38	When placement of the duct is completed and connections of the duct ends are deferred to a later stage, it is advised to overlap duct ends by one meter from each side.
TR 1.39	Both ends of the duct must be properly sealed with end plug to prevent water, dust or any other foreign particle from entering into the duct.
TR 1.40	Pump out water, if any, from the trench before placement of duct.
TR 1.41	Whenever tree roots are found in the trench make sure to lay the ducts under the tree roots and not the above.

TR 1.42	Place the duct along the trench as straight as possible.
TR 1.43	Tightly close the ends of the ducts with self-tightening End Plug so that no dirt, dust or moisture into the duct.
TR 1.44	No spacer will be used however the duct should be tied together with cable tie at an interval of 2 meter positively so as to keep them together.
TR 1.45	**Installation of Plastic Couplers:** • Cut the duct at the same place where they overlap. Cutting should be done in such a way that the duct end matches with each other perfectly because it is very important for the coupling joints to be airtight. • Proper pipe shears or cutters must be used for smooth cutting. Do not use a hacksaw to cut the duct. • Deburr both the inside and the outside edges of the duct with a deburring tool • Apply a small amount of proper lubricant (liquid detergent) for better installation of plastic couplers. • Tighten the plastic coupler with C-Spanner.
TR 1.46	**End Plug:** • Close the ends of duct with end plugs so that moisture, dirt and dust do not enter inside the duct. • It seals the duct ends completely and prevents air, moisture from entering the duct, ever when it is laid underground. • Further interior surface of empty ducts also remains clean even after several years. • Inspect the Neoprene Rubber for various defects such as pin holes, cuts, etc. In case of any such defect, replace the rubber gasket with a new one.
TR 1.47	**Warning Tape:** • This warning tape shall be provided above the telecom duct throughout the route (for open trench only) at a depth of 50% of total trench depth. • Warning tape should be made of HDPE or LDPE (Low Density Poly Ethylene) and other inert material and shall be either bright yellow or orange in colour. • The thickness of tape shall be 1 mm and minimum width 150 mm with life of 25 years. • Neither the colour of tape nor the marking printed inscribed on it shall change or fade away throughout the life time of tape. • The tape should contain a printed message in English “WARNING AITL OFC”.
TR 1.48	**Duct Route Indicators:** • Prefabricated or Precast RCC duct route Indicators are needed to be placed on the Duct Route for open trench. • The route indicator shall be made of RCC material. It shall have embedded on both sides “AITL OFC”. • The route indicator shall be provided based on standard DOT practices. • Route indicators shall be fixed at every 50 meter interval in city area and at both ends of the road crossing for open trench only. • Route Indicator shall be installed at three route layer Viz. Core/Distribution /Access.

Testing: Following testing specific to HDPE duct shall be met. For other testing requirements, refer to the testing section.	
TR 1.49	**Factory Testing Requirements:** • Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. Visual inspection shall be carried out on 100% basis for all the equipment/items offered. Factory acceptance testing shall be carried out on PLB HDPE and accessories. • From each batch PLB-HDPE duct presented by the MSI for Factory acceptance testing, the AITL shall select random sample (s). • The following tests shall be carried out during Factory Acceptance Testing (FAT): ➢ Visual Inspection ➢ Dimension Check ➢ Hydraulic Characteristics ➢ Reversion Test ➢ Tensile Strength and Elongation Test ➢ Environmental Stress Crack Test ➢ Impact Strength Test ➢ Crush Resistance ➢ Mandrel Test ➢ Ovality Test ➢ Coil Set Test ➢ Internal Co-efficient of Friction ➢ Ash content ➢ Colour fading ➢ Optical Fibre Cable Blowing Test ➢ Air Pressure test on plastic coupler ➢ Ageing test on accessories • Dimensional test shall be carried out on 10% sample of the respective lot. • In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected.
TR 1.50	**Duct Integrity Test Procedure:** After laying the Duct network, HDPE ducts shall be tested for proper laying, crush, deformity and pressure testing. The MSI shall have to remove the obstruction/deformity of any kind before handing over of the Duct network to client.
Following tests are to be carried out on the laid HDPE duct:	
TR 1.51	**Duct Cleaning (Sponge Test):** • Compressed air should be blown through the duct in order to remove any dirt and water that has accumulated inside the duct with the help of suitable capacity Air Compressor. • A short blast of air about 2-3 bar shall be blown through the duct for about 2 minutes. • Sponge will be blown through the duct to thoroughly clean the duct from inside.
TR 1.52	**Crush and Deformity Test:** • This test is to be done to check the integrity of the duct. • During installation, while backfilling process there is a possibility of flattening, twisting or kinking of the duct. • This is also possible if the duct has not been uncoiled properly and is laid improperly.

	• Place the wooden shuttle in the duct. Note: Shuttle should be 80% of inner diameter of the duct and 150 mm in length. • Connect the Compressor pipe fitting to the duct. • Place the flexible wire grip to the downstream end of the duct. • Connect the air hose supply to the compressor and the equipment. • Open the discharge valve of the compressor and blow the shuttle through the duct. Note: The shuttle will pass through at a very high speed and must be trapped in flexible wire grip to avoid accident and injury.
TR 1.53	• Mandrel/Shuttle Test – A mandrel/shuttle of at least 90% of the inside diameter size shall be passed through the duct to test the clear pathway of the duct.
TR 1.54	**Pressure Testing:** • This test is carried out to detect leakage in duct, if any. Seal one end of the duct with End Coupler and then through End Coupler with valve, feed the compressed air into the duct. • Raise the pressure upto 5 Bar and then observe. After observing for 30 minutes, pressure drop of upto a max. 0.5 Bar is permissible.
TR 1.55	The detection device for detecting the presence of the buried HDPE Duct with co-extruded copper wire/tracer wire, shall have following features: • One set of Transmitter and Receiver along with suitable batteries in a portable box. • Capability to detect HDPE duct with co-extruded copper/tracer wire wire up to a depth of 3 meters. HDPE duct with co-extruded copper wire is required in all three Network Layers (Core Layer, Distributor Layer and Access Layer). • Capability to emit peak audible signal when the HDPE duct with co-extruded copper wire/tracer wire is exactly below the receiver. • Capability to distinguish presence of passive metallic objects as well as current carrying metallic conductors other than the duct itself. • Capability to indicate the depth of the duct at which it has been buried. • Capability to change the frequency of detection current to avoid possibility of mixing up with detection of another HDPE Duct with co-extruded copper wire/tracer wire in the vicinity, if any. • It should have a backlit LCD display for visibility in low light conditions. • It should have rugged one piece case design and sealed keypad for withstanding tough weather conditions and for superior moisture resistance.
MANHOLE	
TR 1.56	Manholes shall be provided at every finalized location and optical fibre cable service loops.
TR 1.57	Manhole shall be pre cast RCC square type with minimum wall thickness of 100mm and shall include 6mm diameter or more steel reinforcement.
TR 1.58	The bottom of manhole shall be baseless with minimum 100mm thick (Plain Cement Concrete) PCC and minimum internal clearance shall be 1200mm x 1200mm x 1000mm.
TR 1.59	Necessary holes/ cutouts for keeping service loops of duct shall be part of manhole construction.
TR 1.60	All PLB HDPE duct entries, cable entries and holes/ cutouts shall be properly sealed. The holes shall be not more than 6mm larger than the outer diameter of conduit (sleeve). Seal conduit ends inside all manholes with at least 50mm thick duct caulking after fibre is installed. Seal vacant conduit with a manufacturer end plug and attach detectable pull tape.
TR 1.61	The manhole cover shall be heavy duty water tight FRC type. However, for easy handling purpose, the cover shall be constructed with suitable arrangement for lifting.

TR 1.62	All covers shall be manufactured with the markings “AITL OFC MANHOLE” in the logo area of the cover, in 25 mm recessed letters.
TR 1.63	The top of manhole should be flushed with the ground level.
TR 1.64	The manhole shall have suitable excess from cable trench and sufficient holes/ cutouts in all walls for PLB HDPE duct entries and exits.
TR 1.65	Requisite brackets along with cable hangers for placing cable and splice box inside the manhole shall be provisioned and made of junk free material. The splice box shall be mounted vertically on the wall of the manhole.
TR 1.66	All PLB HDPE duct entries, cable entries and holes shall be properly sealed.
TR 1.67	Manholes shall have capabilities to absorb water as per ASTM 570 or applicable BIS standards.
TR 1.68	All manholes shall have grounding halo installed that wraps the manhole and is connected to the ground rod. The halo shall be tin coated, copper ribbon that shall be anchored to concrete approximately 457mm to 610mm apart. The halo shall be bonded to ground rod with non-insulated 6 AWG solid copper conductor.
TR 1.69	The manholes shall be placed on properly compacted surface to ensure uniform distribution of soil pressure on floor.
TR 1.70	Manhole(s) shall be capable of withstanding the required load based on the actual site conditions.
OPTICAL FIBRE CABLE (OFC) OR FIBRE OPTIC CABLE (FOC)	
The Single mode optical fibre shall meet or exceed the following industry standards:	
TR 1.71	ITU-T G.652- Characteristics of a single-mode optical fibre and cable.
TR 1.72	ANSI/ICEA S-87-640-1999 - Standard for Optical Fibre Outside Plant.
TR 1.73	Telcordia GR-20: Generic Requirements for Optical Fibre and Optical Fibre Cable.
TR 1.74	All applicable TIA/EIA standards for single mode fibre cable and those listed in these technical requirements.
TR 1.75	The fibre optic cable shall be single mode, loose tube dielectric armoured cable which shall be ordered in different fibre count and tube configuration as detailed in the functional requirements.
TR 1.76	The single mode optical fibre shall enable dual operating wavelengths at 1310nm and 1550nm nominal. The optical fibre shall be non-dispersion shifted.
TR 1.77	Single mode fibre shall have attenuation not greater than 0.36 dB/km at 1310 nm and 0.25 dB/km at 1550 nm.
TR 1.78	The single mode optical cable shall have the cladding diameter = 125.0µm ±1.0 and Mode Field diameter = 9.0µm ± 0.4.
TR 1.79	The single mode optical cable shall have polarization mode dispersion (PMD) coefficient ≤ 0.2 at 1310nm.
TR 1.80	Fibre attenuation measurements shall be made in the factory in accordance with EIA-455-78A for single-mode fibre. The spectral width of the source used to measure attenuation shall be less than 10 nm.
TR 1.81	When Optical Time Domain Reflectometer (OTDR) is used, measurements shall be made from both directions and the results shall be averaged.
TR 1.82	The attenuation of the single mode fibre shall be distributed uniformly throughout its length such that there are no point discontinuities in excess of 0.1 dB at 1310 nm or 1550nm wavelength. Fibre shall have no voids, air bubbles, or streaks in them. Factory splicing is not permitted. Attenuation Uniformity shall be measured in accordance with EIA-455-59.
TR 1.83	The Chromatic Dispersion of single mode fibre shall be measured in accordance with EIA-455-175 or EIA-455-168.

TR 1.84	The cut-off wavelength of cabled fibre shall be less than 1260 nm. The wavelength shall be measured according to EIA-455-170.
TR 1.85	The single mode fibre optic cable shall be dielectric armoured cable that shall be suitable for outdoor installations, with protection against rodents.
TR 1.86	The minimum bending radius of the fibre optic cable shall be at least 15 times the diameter of the cable or better (static), and shall be at least 10 times the diameter of the cable or better (dynamic).
TR 1.87	Fibre optic cable shall be able to withstand a pulling tension of at least 2700N without any resulting damage.
TR 1.88	The optical fibre coating and/or buffer shall consist of materials that are environmentally stable in order to reduce long term effects of stress corrosion caused by moisture absorption. The coating shall be suitable for removal by industry standard mechanical stripping methods. No chemicals shall be required to strip the coating and/or buffer material.
TR 1.89	Colour coding of individual tubes and fibre shall be in accordance with EIA-598. The fibre colour coding shall be visible throughout the life of the cable. Colour concentrates or inks used to colour the optical fibre shall be heat stable and shall not be capable of permeating through the protective fibre coating causing transmission degradation of the optical fibre.
TR 1.90	All cable shall be supplied on wooden reels, with both ends of the cable accessible for testing. Each reel shall be clearly labelled with the cable code, length, and date of manufacture. All reels shall be protected with solid (2x4) wooden lagging, intended for export shipment.
TR 1.91	Material used in optical fibre cables must not support galvanic action. The core cladding shall be all glass that is predominately silica (SiO_2). Phosphorus, if used as a dopant in the optical fibre, shall be limited to a minimum to reduce the potential effects on fibre attenuation due to hydroxyl ions.
TR 1.92	All fibre optic cables shall be spliced inside dedicated manholes as per the Project requirements. It is the scope of the MSI to provide any additional protection required to the fibre optic cable inside manhole as needed to meet the Project requirements.
TR 1.93	Cable Code and Length Marking shall comply with Telcordia GR-20 standards. This shall include sequentially numbered length markings in meters imprinted on the jacket, and this length marking shall not be reset to zero along the cable length.
TR 1.94	In addition to length markings, each length of the cable must be permanently marked to include the following: • Manufacturer cable and ID code • Year of manufacturer (cable) • Customer Name “AITL” • Number of fibre • SM (single mode)
TR 1.95	Dry water-blocking materials like water swellable tape shall be applied over the cable core to prevent the ingress of water, and movement along the cable sheath.
TR 1.96	Fillers may be included in the cable core to lend symmetry to the cable cross-section where needed. The buffer tubes shall be enclosed in a cable sheath as specified in this section.
TR 1.97	The cabled optical fibre shall maintain mechanical and optical integrity through an operational temperature range of 0°C to +70°C.
TR 1.98	The change in attenuation for single-mode fibre shall not be greater than 0.05 dB/km at 1310 nm and 1550 nm at the operational temperatures limits.

TR 1.99	Temperature cycling measurements shall be made in accordance with EIA-455-3A as per below: • Storage Temperature: 0°C to 60°C • Installation Temperature: 0°C to 55°C • Operating Temperature: 0°C to 70°C
TR 1.100	The cable shall maintain its mechanical and optical performance for an in-service period exceeding 25 years. The MSI shall provide documentation proof to validate this.
TR 1.101	Lightning withstand current shall comply with Telcordia GR-20 standards.
TR 1.102	A sheath slitting cord is required for each sheath.
Installation Requirements:	
TR 1.103	The cable shall support a vertical rise up to 10 m without intermediate cable support.
TR 1.104	The outer jacket of the cable shall be fungus inert and shall be suitable for long term exposure to sunlight and weather.
TR 1.105	Each cable shall be reeled in such a way that both ends of the cable are readily accessible for testing, without any need for unreeling. The inner end of the cable shall be properly secured to prevent whipping when the end of the reel is reached. A minimum of 3 m of the inner end of the cable shall be accessible for optical testing. The inner end must be securely fastened or protected against shipping or installation damage.
TR 1.106	A 10 m slack per cable in every manhole shall be placed along the fibre optic cable route as per AITL requirement.
TR 1.107	Each length of cable shall be wound on a separate cable reel.
TR 1.108	Suitable mechanical pulling aids shall be deployed to ensure that the maximum pulling tension is not exceeded at any time during the installation.
TR 1.109	Tags shall be installed at all cable end points (manholes, etc.).
TR 1.110	The cable shall be neatly dressed, labelled and organized.
Testing: Following testing specific to fibre optic cable shall be met.	
TR 1.111	**Factory Testing Requirements:** • Prior to shipment, Factory-controlled tests shall be performed to verify compliance of the above stated specifications. • Each cable reel shall be shipped with test results indicating the length of the cable reel and the attenuation at 1310 nm and 1550 nm for each fibre, as applicable. A copy of these test results shall also be provided to AITL or their designate. • Any test that reveals the materials or equipment does not meet the stated specifications shall constitute failure. • Visual inspection shall be carried out on 100% basis for all the equipment/items offered. • Dimensional test shall be carried out on 10% sample of the respective lot. • In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected.
TR 1.112	**Pre-Installation Testing Requirements:** • Once delivered to the MSI, the MSI shall, prior to installation, conduct a reel test. • Inspecting for any physical damage of the reel or cable. • Measure using an OTDR, the attenuation at 1310nm and 1550nm for one fibre from each buffer tube from both ends of the cable.

TR 1.113	**Post-Installation Testing Requirements:** • Inspecting for any physical damage of the exposed portions of cable. • Measure using an OTDR, the attenuation at 1310 nm and 1550 nm for every fibre from each buffer tube from both ends of the cable. This includes all connectorized and unconnectorized links with intermediate cable butt splices as applicable. • Inspecting for proper slack loops inside manholes.
TR 1.114	**Mechanical Testing Requirements:** The cable shall meet the following test requirements without physical damage to the cable and/or cable components and without degradation of optical transmission.
TR 1.115	**Crush And Impact Test (Outdoor Cable):** A crush and impact test shall be carried out on a sample of cable approximately 10 m in length according to the method stated in EIA-455-41, and EIA-455-25A /IEC 794. Optical loss measurements are to be made at the 1550 nm nominal wavelength. A permanent or temporary increase in the attenuation loss value greater than 1.0 dB/test-fibre-km shall constitute failure.
TR 1.116	**Twist And Flexibility Test:** A twist and flexibility test shall be carried out on a sample of cable approximately 5 m in length according to the methods stated in EIA-455-85/IEC 794, and EIA-455-104. Optical loss measurements are to be made at the 1550 nm nominal wavelength. A permanent or temporary increase in the attenuation loss value greater than 1.0 dB/test fibre-km shall constitute failure.
TR 1.117	**Water Ingress Test:** A water ingress test shall be carried out on a sample of cable according to the requirements of EIA-455-82A/IEC 794. No water shall leak through the open end of the 1.0m test sample.
TR 1.118	**Certificates And Proof Of Factory Testing:** The bandwidth and attenuation of every fibre in each cable shall be tested in the factory. Single mode measurements shall be taken at 1310 nm and 1550 nm. These factory test results shall be provided with the cable. One copy shall be attached to the cable reel, inside the lagging, prior to shipment, and one copy shall be sent to AITL's Project management office.
UTP COPPER CABLE AND ACCESSORIES	
TR 1.119	The cable shall comprise of four (4) uniformly twisted insulated conductor pairs. Each pair shall have different colour insulation for identification and the two cores of any one pair shall also have different coloured insulation for the identification of a specific core.
TR 1.120	A non-hygroscopic dielectric tape shall be wrapped around the insulated pairs.
TR 1.121	A tight fitting black polyethylene jacket shall be extruded over the shield.
TR 1.122	Conductors shall be twisted to form pairs with an average mutual capacitance of less than 56 nF/km with a far end crosstalk loss of 69 dB/km or better.
TR 1.123	The cable shall have a water repellent filled core and shall have a sunlight and weather resistant jacket of polyethylene (e.g. XLPE). MSI shall propose solution to meet the requirements of the RFQ cum RFP for fulfilling this particular requirement.
TR 1.124	The cable shall have a guaranteed transmission performance upto 250 MHz.
TR 1.125	The cable shall have characteristic impedance of 100 ± 15 (Ohms).
TR 1.126	Materials used in the cable shall not support galvanic action.
COPPER PATCH CORDS	
TR 1.127	Patch cords fabricated from UTP cable shall be of suitable length to connect field devices with the switch/ FTP. Patch cords shall be sized to minimize excess cable interconnecting equipment, with cables routed and dressed to maintain a neat appearance.

TR 1.128	Patch cords shall be terminated with 8-pin 8-conductor “RJ-45” style connectors.
TR 1.129	Pre-fabricated patch cords shall be supplied in individual packages.
TR 1.130	All cabling and connectors shall be in accordance with ANSI/TIA/EIA-568-B.
COPPER PATCH PANEL	
TR 1.131	The copper communication cable shall be terminated at the associated patch panel or field device.
TR 1.132	The patch panels shall be sized to support the design requirements.
TR 1.133	The standard termination is to be according to ANSI/TIA/EIA-568A.
TR 1.134	The termination shall protect the cable terminations from water and mechanical damage and shall be resistant to salt corrosion.
TR 1.135	All material of the termination and associated mounting accessories shall be non-reactive and the complete assembly shall not support galvanic cell action.
TR 1.136	All cable entries shall be provided with appropriate cable pathway.
TR 1.137	Any provided patch panel or wall plate shall provide mechanical support for all connections enclosed and shall maintain insulation between them.
TR 1.138	Connectors shall be sealed water resistant, and shall accommodate the #23 AWG gauge solid conductors. Insulation displacement terminal lugs are permitted.
SURGE SUPPRESSOR	
TR 1.139	Wherever installed, the UTP cables shall be supplied with either in-built surge arrestor or shall have additional surge suppressors.
TR 1.140	Wherever required, Surge suppressors shall be provided and mounted on the active pairs. Two levels of protection shall be provided: • The first protection level shall be a three electrode gas tube discharge protector module. This is only required for cables that leave the cabinet location. • The second level of protection shall be a back-to-back Zener diode arrangement and Metallic Oxide Varistor (MOV). The protection shall be compatible with the first level of protection.
TR 1.141	The surge suppressors shall be such that they do not interfere with normal communications.
FIBRE OPTIC SPLICE CLOSURE (FOSC)	
TR 1.142	Be capable of accepting minimum six (6) cables in a butt splice configuration. Any additional cables shall be supported using standard accessories provided by the manufacturer.
TR 1.143	Fibre Optic Splice Closures shall be IP 68 rating.
TR 1.144	Be re-enterable without the use of additional parts or special materials.
TR 1.145	Not require special tools to enter or assemble.
TR 1.146	Be constructed of non-corrosive materials.
TR 1.147	Have a life expectancy of at least 25 years.
TR 1.148	Be capable of storing up to 3.0m lengths of expressed buffer tubes.
TR 1.149	Accommodate splice organizers which accept heat-shrink fusion protectors or splice protection packs.
TR 1.150	Have provisions for storing Fibre splices and un-spliced Fibre/buffer tubes.
TR 1.151	Be non-filled (no encapsulating material) to prevent water intrusion.
TR 1.152	Meet all performance standards over the operating temperature range of 0°C to +60°C.
TR 1.153	Be capable of preventing a 3.0m water head from intruding into the splice compartment for a period of 7 days, and a 2.0m water head for an indefinite period of time.

OPTICAL CONNECTORS	
TR 1.154	The optical connectors shall comply with Telcordia GR-326-CORE, NWT, American Society for Testing and Materials (ASTM), Telecommunications Industry Association (TIA), as well as Underwriters Laboratories for flammability tests.
TR 1.155	Optical connectors shall conform to the following standards at a minimum: • Small form factor SC and ST/LC • UPC type • Push-on/pull-off interconnection, dry contact, physical contact • Suitable for single-mode installations • Simple polishing tools for infield installation • Available in duplex styles • Connector strain relief limits cable bending radius • Adapters available to mate with other connectors • Insertion Loss < 0.2 dB • Return Loss > -55dB • Repeatability <= 0.1 dB • Thermal Shock <= 0.1 dB • Temperature Cycling <= 0.1 dB 0°C to +60°C (40 Cycles) • Humidity Cycling <= 0.1 dB +60°C (10-95 percent)
FIBRE PATCH CORDS	
TR 1.156	Patch cord material shall conform to the following standards at a minimum: • House a single fibre in a 900 micron tight buffer tube. • House the tight buffer in a flame retardant jacket with space between the jacket and tight buffer filled with Kevlar strength components. • Be available in duplex configurations. • Both mating faces of each connector shall be cleaned using fibre optic cleaning solvent cleaning wipe or patch prior to mating the connector surfaces.
FIBRE DISTRIBUTION AND MANAGEMENT SYSTEM (FDMS)/OPTICAL CABLE ENTRANCE FACILITY (OCEF)	
TR 1.157	The system shall be modular and shall provide compact fibre patching/ splicing system.
TR 1.158	The system shall be fully equipped with necessary accessories such Fan-outs, Fibre Arrangement System, SC/ST/LC connectorised patch cords, 0-dB adapters etc.
TR 1.159	The system shall be able to accommodate all types of optical fibre cable structures.
TR 1.160	The system must guarantee trouble-free extension with no downtime maintenance.
TR 1.161	The system shall have a patch distribution frame with a capacity to meet the Project requirements.
TR 1.162	Each splice tray shall accommodate minimum 24 fibres.
TR 1.163	The system shall have metal housing with movable drawer and integrated fibre management.
TR 1.164	The system shall have a front door with latch for patch cord protection and management.
TR 1.165	The system shall have dedicated cable management and routing to limits bend radius. The cable management could be horizontal or vertical as deemed fit for best performance and shall comply with Industry Standards.
TR 1.166	The system shall have Slack storage in sliding tray to manage and protect excess optical fibre length.
TR 1.167	The system shall be supplied with adjustable mounting bracket available for 19" rack mounting.
TR 1.168	The device shall support operating temperature range of 10°C to +40°C.

FIBRE OPTIC PATCH PANELS / FIBRE TERMINATION PANEL	
TR 1.169	The Patch panels shall adhere to Telecordia GR-449 Core or equivalent specifications.
TR 1.170	The Patch panels shall be capable of supporting SC/ST/LC type ports.
TR 1.171	The Patch panels shall include the mounting hardware for EIA/TIA standard racks as per rack requirements.
TR 1.172	The Patch panels shall provide a minimum of four cable entry points.
TR 1.173	The Patch panels shall support rings to maintain minimum fibre bending radius, and to prevent accidental physical damage.
TR 1.174	The Patch panels shall provide physical protection for the individual fibres.
TR 1.175	The Patch panels shall provide terminating facilities for fibre optic connectors, including the through adapter.
TR 1.176	The Patch panels shall provide a lockable compartment in which fusion splice trays are housed which is separate from the fibre patching area.
TR 1.177	The Patch panels shall provide bulkhead mounting hardware for a variety of connectors but shall be equipped with SC/ST/LC connectors unless otherwise noted.
COMMUNICATIONS CABINETS WITH RACKS	
TR 1.178	Please refer to the Communication Cabinets with Racks specifications mentioned under IT Infrastructure specification Section 2.2.7.3
ACTIVE ELECTRONICS / ETHERNET SWITCHES AND ROUTERS	
Ethernet Switch – Layer 2	
The Layer 2 Ethernet switch includes two types of switches –Type I-Industrial grade switch at field and Type II - Non-industrial grade switch at PoP facility.	
Type I - Industrial Grade Field Switch	
TR 1.179	The Industrial Grade Switch installed at the field shall have at least three (3) 1000BaseTX ports and three (3) 10/100BaseTX ports with two (2) Gigabit Ethernet SFP (1000BaseFX) ports for backhaul (uplink) connectivity. The PoE/PoE+ feature may also be provided via industrial grade PoE/PoE+ injectors for these switches.
TR 1.180	The copper ports shall support PoE / PoE+.
TR 1.181	The industrial grade switches shall support a MAC table size of upto 8000 addresses.
TR 1.182	The industrial grade switches shall at a minimum carry IP30 rating.
TR 1.183	The industrial grade switches shall support – • IEEE 802.3, 802.3ad, 802.3u, 802.3ab, 802.3z, 802.3x protocols. • IEEE 802.1D for STP, 802.1w for Rapid STP, 802.1s for Multiple Spanning Tree Protocols. • IEEE 802.1q for VLAN tagging, 802.1p for CoS, 802.1X for Authentication and 802.3ad for port trunk LACP. • Broadcast storm protection, RADIUS, SSL/SSH security.
TR 1.184	The industrial grade switches shall support – • IPv4/v6, SNMP v1/v2/v3, LLDP, Server/Client, DHCP, TFTP, Telnet, IGMP v1/v2 as a minimum.

TR 1.185	All switches installed on-field shall be capable of working in the harsh environmental conditions with immunity to EMI and heavy electrical surges. They shall support: • EN-60950-1 or Equivalent; • FCC Part 15 Class A All standards to be latest as per Manufacturer's certifications.
TR 1.186	The switches shall be powered by 12/24/48VDC input as per the design requirements with integrated redundant power supply. The terminal blocks for the power supply options shall support reliable, maintenance-free connections. Any power conversions required shall be in the scope of the MSI.
TR 1.187	The industrial grade switches shall support operating temperature range of 0°C to +60°C (without any fans) with ambient relative humidity of 5-95%, non-condensing.
Type II - Non-Industrial Grade Switch	
TR 1.188	These switches shall have at least twenty-four (24) 1000Base-X ports for connectivity to the field devices with at least two (2) 10G Ethernet SFP (10GBase-T/SFP+) ports for inter-switch uplink connectivity.
TR 1.189	The switches shall support a switching capacity of at least 88 Gbps.
TR 1.190	All switches shall support a MAC table size of at least 16,000 addresses.
TR 1.191	The switches shall be powered by 220-240VAC, 50Hz input as per the design requirements with dual redundant hot swappable power supply (in-built) and redundant variable speed fans. Any power supply required for conversion shall be in the scope of the MSI.
TR 1.192	The switches installed inside PoP buildings shall support an operating temperature range of 10°C to +40°C with ambient relative humidity of 10-85%, non-condensing.
General Requirements	
TR 1.193	All Layer 2 Ethernet switches (for Type II only) shall be managed switches and shall comply with the following as a minimum: • IEEE: ➢ 802.3u (fast Ethernet, 100Mbps) ➢ 802.3z (1000BaseFX) ➢ 802.3ab (1000BaseTX) ➢ 802.3x (Full Duplex with flow control) ➢ 802.3ad LACP ➢ IEEE 802.1D MAC Bridges ➢ IEEE 802.1p Priority ➢ 802.1q (VLAN) ➢ IEEE 802.1AB Link Layer Discovery Protocol (LLDP) ➢ 802.1s (multiple spanning tree protocol) ➢ 802.1w (rapid spanning tree protocol) ➢ 802.3ad (port trunking) • Safety: ➢ UL CSA 60950 or equivalent ➢ CAN/CSA-C22.2 No 60950 or equivalent ➢ EN 60950 or equivalent • Electromagnetic emissions: ➢ FCC Part 15 Class A

	• IGMP v1/v2 • TACACS+ and Radius • SNMPv1/v2c/v3
TR 1.194	All Layer 2 switches at a minimum shall support the following: • IPv4/IPv6 • CoS • IP Multicast • Security • Storm Control • Spanning Tree Route Guard • SSH • Network Management • Non-Blocking Type • Support Auto-Sensing • Support Auto-Negotiation
TR 1.195	The fibre optic ports shall support the required distance i.e. between field switch and PoP rooms.
TR 1.196	All switches shall support standard 19" rack mount.
TR 1.197	All switches shall have the function to enable/disable ports for limiting unauthorized access to the network.
TR 1.198	All switches shall support Network Time Protocol (NTP) for time synchronization.
TR 1.199	All switches shall support multilevel user passwords for prevention against unauthorized configuration.
TR 1.200	All switches shall support SSH/SSL based security and MAC based port security.
TR 1.201	All switches shall support RADIUS authentication service.
TR 1.202	The device shall have LED indicators for Power, LAN and ports.
TR 1.203	All switches shall have a Mean Time Between Failure (MTBF) of at least 200,000 hours.
Ethernet Switch & Router – Layer 3	
The Layer 3 Ethernet switch/router includes three types –Type I-Backbone Ethernet switch/router, Type II – Core router, and Type III – Server/workstation connectivity Ethernet Switch.	
Type I - Backbone Ethernet Switch/Router	
TR 1.204	The Layer 3 based backbone Ethernet switch/router shall be installed for backbone connectivity between PoP to PoP and between Mini Control Centre (MCC).
TR 1.205	The Layer 3 based backbone Ethernet switch/router shall have minimum 8 SFP+ ports with 10 Gb/s connectivity including Copper/ /Fibre ports (for backhaul between PoPs and MCC) as per the design requirements and scalable to additional 4 SFP+ 10 Gb/s ports. These ports shall support hot swap modules to support upgrade of ports in the future. It is expected that at least 2 ports per switch shall support Copper port/Fibre Ports configuration for inter-switch connectivity. Any attenuators required for inter-switch connectivity shall be provided by MSI.
TR 1.206	The backbone switch/router shall have a minimum switching capacity of 128 Gbps, non-blocking.
TR 1.207	The backbone switch/router shall support IP/MPLS connectivity and shall be carrier grade.
Type II – Core Router	
TR 1.208	The core router shall be installed at the PoP/MCC for connectivity to outside world.

TR 1.209	The core router shall have a minimum throughput of 40 Gbps per slot. Core router shall be as per Bidder's overall solution and meeting the overall throughput requirements.
TR 1.210	The core router shall have multiple = 10 Gigabit Ethernet Small Form-Factor Plus Pluggable (SFP+) ports with following interfaces: 10 Gigabit Ethernet, 1 Gigabit Ethernet.
Type III – Server/Workstation Connectivity Ethernet Switch – Minimum 24 Ports	
TR 1.211	The Layer 3 based Ethernet switch shall be installed for connectivity to servers and workstations at MCC and PoP.
TR 1.212	The Layer 3 based Ethernet switch shall have a minimum of 24 ports (at least 50% spare) Ethernet interface with a combination of 1/10 Gig SFP+ ports.
Common Requirements – Switch/Router	

TR 1.213	All Layer 3 switches/routers shall comply with
	• IEEE:
	  ➢ 802.3u (fast Ethernet, 100Mbps)
	  ➢ 802.3z (Gigabit Ethernet)
	  ➢ 802.3ae (10 Gigabit Ethernet)
	  ➢ 802.3x (Full Duplex with flow control)
	  ➢ 802.1q (VLAN)
	  ➢ 802.3p (CoS)
	  ➢ 802.1d (spanning tree protocol), 802.1w (rapid spanning tree protocol) and 802.1s (multiple spanning tree protocol)
	  ➢ 802.3ad (link aggregation control protocol)
	  ➢ 802.3 (Management)
	• IPv4/v6IGMP v1/v2/v3;
	• Routing Information Protocol v2 (RIPv2), Open Shortest Path First Version 3 (OSPFv3), Border Gateway Protocol (BGP) Version 3, and Intermediate System-to-System (IS-IS)
	• Policy based routing;
	• Multicast;
	• Per port QoS configuration;
	• Safety:
	  ➢ EN/IEC/UL CSA 60950-1
	• Electromagnetic emissions:
	  ➢ FCC Part 15 Class A

TR 1.214	All layer 3 switches/routers shall support IP/MPLS based networking.
TR 1.215	All switches/routers shall support standard 19" rack mount or DIN rail mounting options.
TR 1.216	All interfaces shall be modular.
TR 1.217	The switches/routers shall support at least one (1) dual personality port (RJ-45 or USB micro-B) serial console port.
TR 1.218	The switches/routers shall be supported with LED indicators for easy troubleshooting.
TR 1.219	The switches/routers shall support operating temperature range of 10°C to +40°C with ambient relative humidity of 10-85% non-condensing.
TR 1.220	The backbone switches/routers shall be powered by 220-240VAC, 50Hz input as per the design requirements with hot swappable dual redundant power supply (in-built) and redundant variable speed fans.

TR 1.221	All switches/routers shall have a Mean Time Between Failure (MTBF) of at least 100,000 hours.
General Requirements – Core Router	
TR 1.222	The core router shall be chassis based with modular architecture for scalability with Redundant - Route Processor, Power supply, Switching fabric; and shall deliver multiple IP services over a flexible combination of interfaces.
TR 1.223	Shall support Network Interface module.
TR 1.224	The core router shall have a total switching capacity of at least 200 Gbps, non -blocking.
TR 1.225	The core router shall be support standard TIA/EIA 19" rack mounting.
TR 1.226	The core router shall support 4000 multicast routes.
TR 1.227	The core router shall support both IPv4 and IPv6 policy based routing.
TR 1.228	The core router's management functionality shall be greater than SNMP v2.
TR 1.229	The core router shall have event and system history logging capabilities. The Router shall generate system alarms on events and capable of log analysis.

TR 1.230	The core router at a minimum shall support the following protocols:
	• IPv4/IPv6
	• QoS/CoS
	• IP multicast
	• General:
	  ➢ IEEE 802.1D MAC Bridges
	  ➢ IEEE 802.1p Priority
	  ➢ IEEE 802.1Q VLANs
	  ➢ IEEE 802.1s Multiple Spanning Trees
	  ➢ IEEE 802.1w Rapid Reconfiguration of Spanning Tree
	• Security:
	  ➢ RFC 1492 TACACS+
	  ➢ RFC 2138 RADIUS Authentication
	  ➢ RFC 2866 RADIUS Accounting
	  ➢ Secure Sockets Layer (SSL)/ SSH
	• Network Management:
	  ➢ IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
	• RFC 3031 MPLS (Multi-Protocol Label Switching)
	• RFC 1098 A Simple Network Management Protocol (SNMP)
	• RFC 2819 Four groups of RMON: 1 (statistics), 2 (history), 3 (alarm) and 9 (events)
	• ANSI/TIA-1057 LLDP Media Endpoint Discovery (LLDP-MED)
	• SNMPv1/v2c/v3

TR 1.231	The core router shall be powered by 220-240VAC/50Hz input as per the design requirements. Any power converters required shall be under the scope of the MSI.
TR 1.232	The core router shall support N+1 hot swappable redundant power supply module with redundant fan modules.
TR 1.233	The core router shall comply with the following standards: • FCC 47 CFR Part 15 Class A; • ICES-003 Class A;

	• EN55022/CISPR 22 Information Technology Equipment; • Immunity: EN300 386 Telecommunications Network Equipment; • EMC: EN50082-1/EN61000-6-1 Generic Immunity Standard; • Safety: UL60950-1; CSA C22.2 No. 60950; EN 60950-1; IEC 60950-1;
NETWORK MANAGEMENT SYSTEM (NMS)	
TR 1.234	The NMS shall have an integrated user-friendly application.
TR 1.235	The NMS shall include all required licenses and shall be scalable for management of service provider configurations.
TR 1.236	The NMS shall provide real-time monitoring of the entire network infrastructure and shall allow users to easily navigate with graphical interface and easy to use network management tools.
TR 1.237	The NMS shall provide at a minimum, event alert via the existing Microsoft Exchange Server email or pop-up alarm or export to CSV.
TR 1.238	The NMS shall automatically generate reports on a daily, weekly and monthly basis in formats including graphs, bar charts, distribution and summary. The system shall be capable of printing out reports and also exporting the reports to other systems or web servers.
TR 1.239	The NMS shall display a simple map of the whole network as a tree and shall have the option of direct selection of objects. The system shall provide a navigation tree to display the current alarm status of each subnet. All the system shall support PAN/ ZOOM feature and shall have all the devices visible in one window along with the provision for these two features.
TR 1.240	The NMS shall provide polling agents to upload status, changes or alerts of the local devices attached with the Ethernet enabling devices.
TR 1.241	The NMS shall provide real time Management Information Bases (MIBs) displays and shall provide the MIB variable data in tabular or graphical format. The MIB displays shall provide various expressions like utilization, percentage errors and volume.
TR 1.242	The NMS shall provide features for security and accountability and shall generate a log file for any user access to configuration or platform changes.
TR 1.243	The NMS shall be capable of managing any SNMP/ICMP device from any vendor.
TR 1.244	The NMS shall support SNMPV1, SNMPV2C and SNMPV3 and shall automatically discover and poll SNMP and ICMP devices.
TR 1.245	SNMP traps for all IP enabled devices shall be provided by the respective product manufacturers.
TR 1.246	The NMS shall allow notifications to be automatically sent to phones, offsite workstations, etc. for efficient response.
TR 1.247	The NMS shall monitor as a minimum the base station units and the subscriber station units along with other IP enabled equipment that is being provided as part of this Project.
TR 1.248	The NMS shall allow for providing different levels of security access i.e. viewing, logging and managing.
TR 1.249	The NMS shall allow for display different colours for the links including red, green, orange, yellow to show the status of the links and the connected devices.
TR 1.250	The operation of the NMS shall be tested while the backbone network is under 30% network utilization.
TR 1.251	The NMS shall have secure wired and wireless guest access that provision controlled wireless access to tenants, while keeping the network secure.
TR 1.252	The NMS shall have role-based access control provides flexibility to segment the wireless network into one or more virtual domains controlled by a single management platform.

TR 1.253	The NMS must provide an interface for IT helpdesk personnel to create guest credentials.
TR 1.254	The NMS shall be supplied with a server with Windows or Linux based OS (latest) or later and a workstation. • For NMS Server Specifications, Please refer to the Server specifications mentioned under IT Infrastructure specification Section 2.2.7.4 • For NMS Workstation Specifications, Please refer to the Workstation specifications mentioned under IT Infrastructure specification Section 2.2.7.2
POINT OF PRESENCE (PoP)	
TR 1.255	PoP design shall at a minimum meet the following reference standards: • NBC (National Building Code), 2005 • DoT guidelines for arrangement & installation of telecommunication equipment inside & outside building. • TEC norms for basic infrastructure of internal & external communication network.
TR 1.256	**General:** • The PoPs shall include both primary and secondary PoP facilities. These facilities shall act as co-location spaces for both AITL and non-AITL (tenants) needs. • The Primary PoP will also act in a Secondary PoP capacity as a termination point for distribution fibre that connects to the plots located within its immediate vicinity. • All TSPs including cellular service providers along with other tenants shall terminate their equipment inside the PoPs. It is expected that at one of the PoPs, the TSPs will terminate their fibre from outside Bidkin. • All AITL owned fibre optic infrastructure shall originate and terminate at the PoPs with dual entry-exit redundant paths. • The PoPs shall have sufficient space for UPS for AITL infrastructure. The TSPs shall be given only bare shell space with partition i.e. dedicated space. The TSPs shall be responsible for any additional active infrastructure required inside their respective space. • Each room shall have provision of underfloor raceway/ trench for access of communication/ emergency electrical supply (UPS supply) as per the standard practice of arrangement for equipment racks. • Each room shall have provision of electrical and In-Out cable access of outdoor unit for air conditioning of required capacity with 100% redundancy as per TEC norms. • All PoP rooms shall have an industry standard rodent repellent system.
TR 1.257	**Building Construction:** • Air filtration efficiency in accordance with ASHRAE 52.1 telecom industry standards. • HVAC shall be designed in such a way that the operating temperature is maintained at average 23 degrees C with spot minimum of 18 degrees C and spot maximum of 26 degrees C. Humidity shall be in the range of 40-60% RH. This shall be applicable for the AITL area only and include full redundancy. • All PoPs shall include industry standard fire detection systems. In addition, the AITL room at each PoP i.e. approximately 100 sq.ft shall also include gas suppression systems. • All cabling and pathways within the PoPs shall be fire stopped only. • Average lux level across all spaces (internal) in PoP rooms shall be 300. Only LED lights shall be used to meet the lighting requirements of the PoP facility.
TR 1.258	**Electrical:** • PoP rooms shall have redundant electrical feeds for power. This shall be coordinated with the EPC Contractor. In-coming power shall be tapped by the MSI from the nearest tapping point. Associated electrical panel at the PoP shall also be provided by the MSI.

	• Each suite/tenant shall have separated metered power, supplied from the main electrical panel located in the AITL suite (tenant to provide their own meter), while for AITL, MSI shall provide this meter. • All electrical wiring, switch, sockets, etc. used for internal/ external building electrification shall be certified by Indian standards under grade-A and fulfil the requirement of ECBC guidelines. • Separate wiring shall be laid for UPS supply and wiring shall be interface at distribution board/ Panel board with main supply. • In case of Raceway, separate raceway shall be provide for electrical cable/wiring. • Air conditioning points rating shall be confirmed as per the required capacity of room.
TR 1.259	**Communication:** • MSI shall provide the access of OFC and RF cables for cellular tower to each TSP room and other tenant rooms as per the design requirements. • MSI shall provide the dedicated raceway/ trench inside the building for entire communication network. • All raceway/ trench shall be properly sealed to protect water, dust etc. from outside and have suitable opening wherever required to operation & maintenance. • Trench/ raceway layout plan shall be furnished by MSI and submit to AITL for their review & approval. • MSI shall follow the recommendation of AITL and local telecom authority to freeze the location & height of communication points.
ENTERPRISE MANAGEMENT SYSTEM (EMS)	
Availability - Monitoring, Management and Reporting	
TR 1.260	The proposed system shall support multiple types of discovery like IP range discovery – including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices.
TR 1.261	The proposed system shall support exclusion of specific IP addresses or IP address ranges.
TR 1.262	The discovery shall be able to identify and model of the ICT asset.
TR 1.263	The proposed system shall provide a detailed asset report, organized by proper naming of all devices, listing all ports for all devices. The proposed system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.
TR 1.264	The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason.
TR 1.265	The proposed system shall provide out of the box root cause analysis.
TR 1.266	Proposed EMS system shall also perform Proactive monitoring (for applications) of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnosis.
Service Level - Monitoring, Management and Reporting	
TR 1.267	The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the component and services provisioned as well as the SLAs.
TR 1.268	The system shall provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
TR 1.269	The system shall be capable of managing IT and Non-IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.

TR 1.270	The Service Level Agreements definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, quarterly, etc.).
TR 1.271	SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated. These alarms shall be automatically shared with the authorized people.
TR 1.272	The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition the capability to exempt any service outage from impacting an SLA shall be available.
TR 1.273	The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
TR 1.274	The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
Application Performance - Monitoring, Management and Reporting	
TR 1.275	The proposed solution shall proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.
TR 1.276	The proposed solution shall determine if the cause of performance issues is inside the application, in connected back-end systems or at the network layer.
TR 1.277	The proposed solution shall correlate performance data from HTTP Servers (external requests) with internal application performance data.
TR 1.278	The proposed solution shall see response times based on different call parameters. For example the proposed solution shall be able to provide CPU utilization metrics.
TR 1.279	The proposed solution shall allow data to be seen only by those with a need to know and limit access by user roles.
TR 1.280	The proposed solution shall measure the end users' experiences based on transactions.
TR 1.281	The proposed solution shall give visibility into user experience without the need to install operators on user desktops.
TR 1.282	The solution shall be deployable as an appliance-based system acting as a active/passive listener on the network thus inducing zero overhead on the network and application layer.
TR 1.283	The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.
TR 1.284	The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction.
TR 1.285	The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the Data centre without having to rely on network monitoring tools.
TR 1.286	The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time. Reports and dashboards shall also be role-based so that business and IT stakeholders get the necessary visibility into the health of business and also provide out-of-box KPIs that can be used to present different aspects of business service health.
Systems and Database Performance - Monitoring, Management and Reporting	
TR 1.287	The proposed system shall addresses management challenges by providing centralized management across physical and virtual systems.

TR 1.288	The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using operators on the servers to be monitored.
TR 1.289	It shall be possible to configure the operating system monitoring operators to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
TR 1.290	It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the operators and setting thresholds.
TR 1.291	The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
TR 1.292	The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started.
TR 1.293	The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to take action like sending an email.
TR 1.294	The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
TR 1.295	It shall be able to automate monitoring, data collection and analysis of performance from single point.
TR 1.296	It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling Database Administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.
TR 1.297	Role based Access — Enables role-based management by defining access privileges according to the role of the user.
TR 1.298	The proposed Virtual Performance Management system shall integrate latest virtualization technologies.
Helpdesk - Monitoring, Management and Reporting	
TR 1.299	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.
TR 1.300	The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.
TR 1.301	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.
TR 1.302	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
TR 1.303	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.
TR 1.304	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.
TR 1.305	The proposed helpdesk system shall have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues.
TR 1.306	The proposed helpdesk system shall support tracking of SLA (Service Level Agreements) for call requests within the help desk through service types.

TR 1.307	The proposed helpdesk system shall be capable of assigning call requests to tech al staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.
TR 1.308	The proposed helpdesk system shall integrate tightly with the knowledge tools and CMDB and shall be accessible from the same login window.
TR 1.309	It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
TR 1.310	Remote desktop sharing in the system shall be operator less & all activity shall be automatically logged into the service desk ticket.
TR 1.311	It shall allow IT team to create solution & make them available on the end – user login window for the most common requests.
Traffic Analysis through EMS	
TR 1.312	The traffic analysis system shall be from same OEM providing Network Fault & Performance Management System.
TR 1.313	The tool shall support Flow monitoring and traffic analysis for NetFlow, J-Flow, sFlow, Netstream, IPFIX technologies.
TR 1.314	The solution shall provide a central web based integration point across any of the flow protocols and shall be able to report from a single console across at least 20,000 interfaces.
TR 1.315	The solution shall be of passive type and should not cause any performance overheads.
Incident Management and Root Cause Analysis Reporting	
TR 1.316	An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management policy.
TR 1.317	Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.
TR 1.318	It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.
TR 1.319	Testing shall be performed to ensure that recovery action is complete and that the service has been fully restored.
TR 1.320	When the incident has been resolved, it shall be ensured that the service desk records of the resolution steps are updated, and confirm that the action taken has been agreed to by the end user. Also, unresolved incidents (known errors and workarounds) shall be recorded and reported to provide information for effective problem management.
TR 1.321	Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
TR 1.322	Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
Change and Configuration Management	
TR 1.323	Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.

TR 1.324	All changes shall be initiated using change management process; and a Request For Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.
TR 1.325	All changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes.
TR 1.326	Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change shall be analyzed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.
TR 1.327	Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
TR 1.328	The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.
TR 1.329	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.
TR 1.330	The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access.
TR 1.331	The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.
TR 1.332	Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.
TR 1.333	Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.
TR 1.334	A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.
TR 1.335	Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, software and hardware configuration images.

2.2.2 Public Wi-Fi

2.2.2.1 Overview

Public Wi-Fi shall be one of the key service offerings by AITL to its citizens; an initiative aimed to enable mobile broadband to be affordable, accessible and available for citizens. The Wi-Fi infrastructure shall comprise of a combination of Wi-Fi Access Points (APs), mounting infrastructure, and associated active and passive infrastructure including fibre/copper based network.

Similar to AURIC-Shendra, AURIC-Bidkin will be a Greenfield smart city which will have a considerable number of workforce and population. Hence, there is a requirement to provide Wi-Fi services across all public spaces and other strategic locations for enabling the mobile broadband to be affordable, accessible and available for its citizens. Through this approach, AITL will be able to offer Wi-Fi as a service to its citizens across AURIC.

In addition to citizen benefits, the presence of a public Wi-Fi network shall be able to draw multiple benefits for the AITL workforce. AITL employees will also utilize the benefits of mobile connectivity for m-governance applications throughout AURIC-Bidkin, allowing efficient access to mobile applications that support their individual work processes, from building inspections to solid waste removal, and municipal services. Any municipal function that requires employees to be mobile shall benefit from the Wi-Fi connectivity. Financially, this will reduce the costs for cellular data (3G/ LTE) that AITL will be paying as almost all mobile data will flow across the city Wi-Fi network. Moreover, Wi-Fi shall also be used for offering e-governance services for the citizens.

For the implementation of a city Wi-Fi network, following are the two (2) types of infrastructure being proposed for Wi-Fi Access Points:

- Outdoor Rated Access Point (AP) co-located on Street Light Poles: This setup shall be used across all public Right of Way (RoW) areas;
- Integrated with Multi-Services Digital Kiosk: Wi-Fi access points shall be integrated within the Multi-Services Digital Kiosk that will be installed at strategic locations across AURIC-Bidkin Phase-1 such as parks and other public spaces.

2.2.2.2 Architecture

The approach for Wi-Fi is that AITL will invest in building the Wi-Fi infrastructure including access points and associated hardware and software, and will provide fibre to each of the access points for backhaul purposes. However, the MSI will have a neutral operator responsible for operating the Wi-Fi network and will also be responsible for providing the raw bandwidth for the Wi-Fi network. This neutral operator will act as an operator of operators, i.e. tenant based model who in-turn will offer Wi-Fi services from various telecom service providers. MSI can offer additional value-add services such as music, videos, games etc. over this Wi-Fi LAN network and can also use this network for 3G/4G offloading.

The Wi-Fi APs and Multi-Services Digital Kiosks will be connected using dedicated fibre optic infrastructure. Each of the Wi-Fi APs will have dedicated fibre counts that will connect back to the nearest PoP. For redundancy, the AP shall use wireless frequency for creating a mesh to ensure continuous communications in case of a fibre link not being available.

Wi-Fi network shall also include a Wi-Fi management software and application with a secure login procedure. The city Wi-Fi network shall also support mobility i.e. people driving or walking within AURIC-Bidkin will be able to access the Wi-Fi network on the move for within the coverage area as per the project requirements.

The overall concept of operations for city Wi-Fi is such that AITL will provide Wi-Fi as a service to its citizens. It will allow citizens to use Wi-Fi for various e-governance applications, use Wi-Fi with a one-time login, coupon based login or premium plan. The summary of the overall concept of operations in terms of different services being offered via the city Wi-Fi network are:

- One-time login – each session will last for 30 minutes or 100MB (whichever happens first) post which the user will have to go through the login process again;

- AURIC city services, i.e. e-governance and m-governance – all e-governance and m-governance services to be offered to citizens and AITL employees using the Wi-Fi LAN at no cost to the citizens for any amount of time;
- Plans – various coupons will be available for using the city Wi-Fi services. These coupons will be made available at strategic locations across Bidkin including Multi-Services Digital Kiosk. Further, they can also be available via SMS service. In addition, there will be premium plans available to the citizens for:
  - Purchasing a premium plan session at one time that lasts more than 30 minutes or 100 MB and/or at a faster speed. This plan shall be applicable throughout Shendra and Bidkin (AURIC);
  - Extended dwelling plan – It is expected that the Wi-Fi operator is neutral and allows multiple Internet Service Providers (ISPs) to offer their services using this Wi-Fi network. As part of the Project, it is expected that there will be some ISPs who also offer wired broadband services. Therefore, there will be an option for the user to extend the wired broadband service plan at the dwelling to city Wi-Fi service by paying a premium over the base plan that is being used by the user.

The overall indicative process flow for the city Wi-Fi network has been presented as part of the Exhibit 6 below.

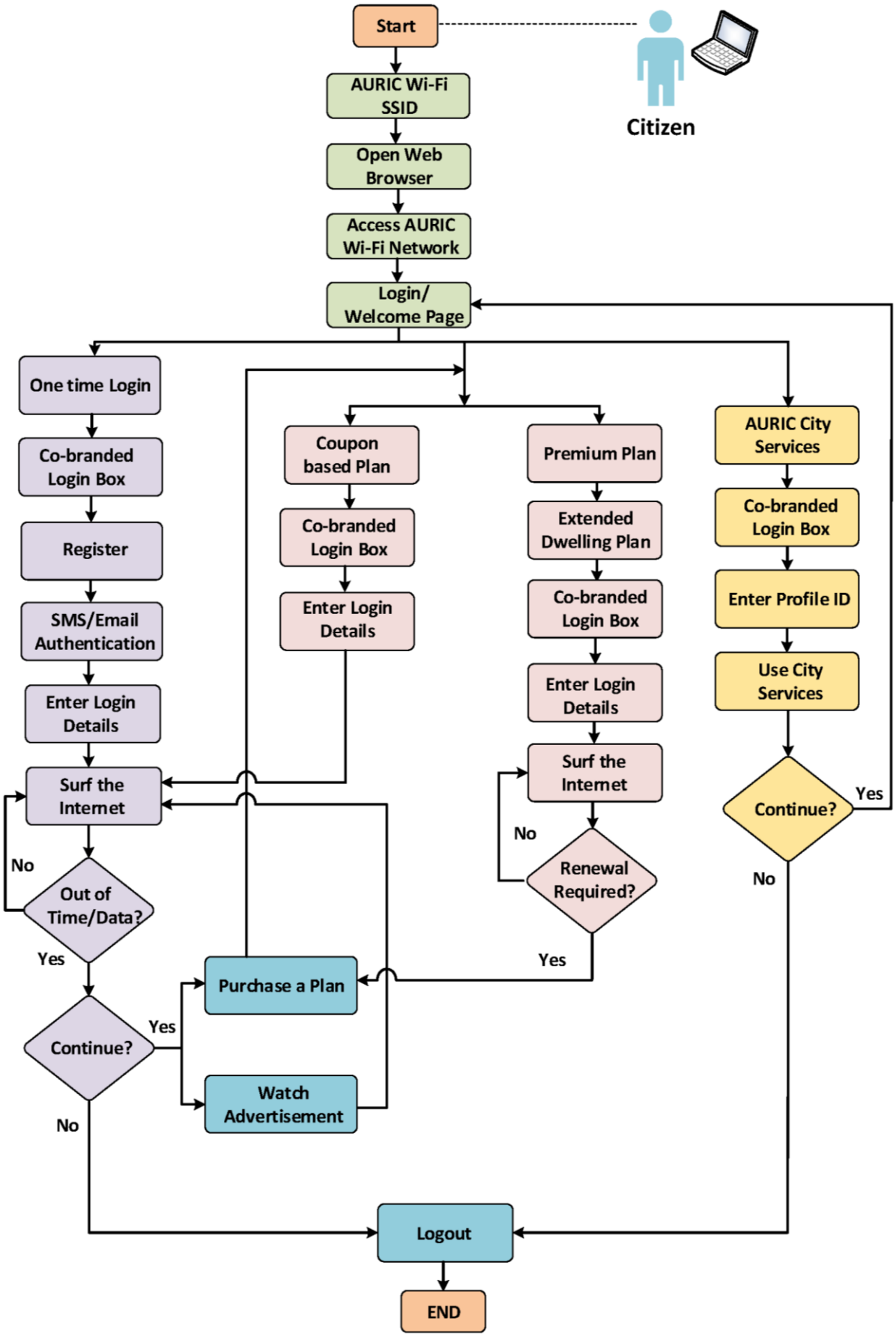


Exhibit 6: Process Flow for the City Wi-Fi Network

BR - 2 Business Requirements

BR 2.1	Wi-Fi shall be one of the key service offerings by AITL to its citizens.
BR 2.2	Wi-Fi is an initiative aimed to enable the mobile broadband to be affordable, accessible and available for the citizens.
BR 2.3	Wi-Fi shall be used for offering e-Governance services for the citizens and m-governance services to AITL workforce. For municipal functions and e-Governance services, the Wi-Fi services shall be free of charge.
BR 2.4	Wi-Fi shall be provided at no cost to the user for 30 minutes or 100 MB (whichever happens earlier) at 4 Mbps download per user per session. Post this, custom plans can be created for the user based on consultations with the Client.
BR 2.5	Wi-Fi services shall be provided using a neutral operator i.e. an operator who supports multiple ISPs (tenant based model) to offer their services through the AITL infrastructure. Further, 3G/4G offload can also be supported using city Wi-Fi network.
BR 2.6	Beyond the free Wi-Fi services for citizens, the Master System Integrator (MSI) that will be appointed, may monetize the Wi-Fi services without impacting the overall user experience and in consultation with the Client. The MSI will retain all monetization derived from the city Wi-Fi services.
BR 2.7	Wi-Fi services shall support the extended dwelling plan option i.e. extend a user's personal broadband connection across AURIC.
BR 2.8	MSI at his own cost may offer Wi-Fi as a service to any plot holder within the plot or building after getting consensus with the Client.
BR 2.9	Wi-Fi services shall be offered in compliance with the regulations and policies from both TRAI and DOT.
BR 2.10	Wi-Fi Operator shall be a Licensed ISP in India who shall be able to meet all requirements for operations of network.
BR 2.11	Wi-Fi network shall be integrated with payment gateway (provided by AITL) and coupon based system for payments by the users for browsing.
BR 2.12	Contention ratio shall be assumed as 200:1 for the Wi-Fi services.

FR - 2 Functional Requirements

GENERAL	
FR 2.1	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
FR 2.2	Wi-Fi shall have a secure, seamless and redundant network. It shall support industry standard based two (2) step authentication procedure.
FR 2.3	Wi-Fi services shall be provided across all public spaces and other strategic locations in consultations with the Client.
FR 2.4	The target bandwidth proposed per end-user is 4 Mbps throughout the City on a per session basis for the 30 minutes or 100 MB per session that will be given to the user at no cost.

FR 2.5	The system shall be designed for scalability and allow future expansions in terms of subsequent project phases, increased user density and geographical coverage.
FR 2.6	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.
FR 2.7	All AITL promotions can use the Wi-Fi network without any cost.
FR 2.8	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.
FR 2.9	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	
FR 2.10	For the implementation of a city Wi-Fi network, the following are the two (2) types of infrastructure being proposed for Wi-Fi Access Points: • Outdoor Rated Access Point (AP) co-located on Street Light Poles: This setup shall be used across all public right-of-way areas. • Integrated with Multi-Services Digital Kiosk: Wi-Fi access points shall be integrated at the Multi-Services Digital Kiosks installed at the strategic locations within the plots.
FR 2.11	The access points shall be capable of managing and configuring remotely through a wireless controller.
FR 2.12	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.
FR 2.13	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.
FR 2.14	Access Point and Multi-Services Digital Kiosks shall be connected using dedicated fibre optic infrastructure for backhaul to Point of Presence (PoP).
FR 2.15	The Wi-Fi access point shall be controller based that can be managed by using Wi-Fi controller at Mini Control Centre (MCC) and ACC.
FR 2.16	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	
FR 2.17	Wi-Fi network shall include Wi-Fi controller to monitor, manage, and control access points from the MCC and ACC.
FR 2.18	The controller shall ensure seamless roaming within AURIC-Bidkin.
FR 2.19	The controllers should communicate back and forth with the centralized security system and network management system in real time.
FR 2.20	The controller shall have inbuilt wireless intrusion protection capabilities.
WI-FI MANAGEMENT SYSTEM	
FR 2.21	The Wi-Fi shall also include a Wi-Fi management software and application with a secure login procedure.
FR 2.22	Wi-Fi Management System shall be a centralized system to monitor, analyze, 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 MCC.

FR 2.23	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 static optimizing the network for the next day.
FR 2.24	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.
FR 2.25	Database: The system shall have a centralized database and subscriber management system.
FR 2.26	The Wi-Fi network shall support multiple BSSIDs as needed to support the overall concept of operations including support for multiple operators.
FR 2.27	Fully redundant Authentication, Authorization, and Accounting (AAA) services with OTP/password shall be provided to support city wide services.
FR 2.28	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 AITL's systems.
USER LOGIN AUTHENTICATION PLANS	
FR 2.29	Beyond the 30 minutes or 100 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.
FR 2.30	Industry standard two (2) step authentication shall be required for all sessions.
FR 2.31	iOS and Android applications to be given for seamless connectivity to network-Auto-detect/ Auto-login.
FR 2.32	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.
FR 2.33	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 AURIC city.
FR 2.34	Users shall have an option to enable/ disable connection to city Wi-Fi.
FR 2.35	Users shall also get prompts and alerts for excess data usage.
FR 2.36	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.
FR 2.37	AITL shall be able to generate MIS report to view overall usage, collections and other usage statistics over a defined time period.
ENCRYPTION AND SECURITY	
FR 2.38	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.
FR 2.39	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.
FR 2.40	Wi-Fi network shall support Protected Extensible Authentication Protocol (PEAP) protocol.
FR 2.41	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.
FR 2.42	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.
FR 2.43	The Wi-Fi Network shall support BSSID based IEEE 802.1x authentication and accounting.
FR 2.44	The Wi-Fi network shall support MAC based authentication to provide simple authentication based on users MAC address.

TR - 2 Technical Requirements

GENERAL	
TR 2.1	The Wi-Fi access points shall be co-located on Street Light Poles and mounted on the Multi-Services Digital Kiosks.
TR 2.2	The Wi-Fi central hardware and software shall be installed at the MCC.

TR 2.3	• Organization IEEE:
	  ➢ IEEE 802.11a/b/g/n/ac;
	• Organization European Standard (EN):
	  ➢ EN50121-1 EMC or UL/IEC/EN 60950;
	• Organization Underwriters Laboratory and IEC;
	• Department of Telecommunications guidelines;
	• Telecom Regulatory Authority of India guidelines.

ACCESS POINT	
TR 2.4	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.
TR 2.5	The Wi-Fi access point shall be supplied with omni-directional antennas 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.
TR 2.6	The Wi-Fi access point shall have a built-in spectrum analyser capable of part-time or dedicated spectrum analysis to identify sources of RF interference either built-in or as part of the overall solution.
TR 2.7	The Wi-Fi access point shall be controller based that can be managed by using Wi-Fi controller at MCC which will further be integrated to ACC.
TR 2.8	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.
TR 2.9	The Wi-Fi access point shall provide the fastest and highest throughput with lowest latency even in the most challenging RF environment.
TR 2.10	The Wi-Fi access point shall support dual frequency as authorized by DoT.
TR 2.11	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.
TR 2.12	The Wi-Fi access point shall have multiple SSIDs with QoS and security policies.
TR 2.13	The Wi-Fi access point shall allow setting up of configurable speeds per user and configurable number of users. It shall support upto 200 concurrent users at any time.
TR 2.14	The Wi-Fi access point shall support reliable multicast video to maintain video quality.
TR 2.15	The Wi-Fi access point shall also support additional features for AITL staff members as needed using a separate secure SSID. Each AP shall support at least 16 different BSSIDs.
TR 2.16	The Wi-Fi access point shall support 20 MHz, 40 MHz, and 80 MHz channelization.
TR 2.17	The Wi-Fi access point shall be IEEE 802.3af/at Power over Ethernet (POE)/POE+ compliant.
TR 2.18	The Wi-Fi access point shall support: • Minimum One PoE+ autosensing port 10/100/1000BASE-T Ethernet network interface (RJ-45). • Power over Ethernet (PoE) or Power over Ethernet+ (PoE+).

TR 2.19	The Wi-Fi access point shall have LED based visual indicator for: • Power/System status • Link status
TR 2.20	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.
TR 2.21	The Wi-Fi access point shall be IP67 compliant and NEMA 4X rated.
TR 2.22	The Wi-Fi access point must support IPV4 and IPV6.
TR 2.23	The Wi-Fi access point shall support telnet and/or SSH login/ console for troubleshooting.
TR 2.24	The Wi-Fi access point shall be reliable ensuring fast, dependable bandwidth and industry standard encryption for security.
TR 2.25	The Wi-Fi access point shall independently be configurable to handle security, mesh, WIPS (either in-built or part of overall solution), RF Management, QoS, roaming, local forwarding without the need for a controller so as to increase performance of the WLAN network.
TR 2.26	The Wi-Fi access point shall be supplied with OEM mounting kit and shall support pole mounting option.
WI-FI CONTROLLER	
TR 2.27	The controller shall support 802.11a/b/g/n/ac.
TR 2.28	Each controller shall support 500 access point nodes at a minimum and shall be scalable as and when required up to 1000 access point per controller.
TR 2.29	The Controller shall support redundancy feature i.e. Active: Active and Active: Standby features. Same licence shall be shared by the controllers.
TR 2.30	The controller shall support centralized or distributed traffic forwarding architecture.
TR 2.31	The controller shall ensure a high throughput even in the most challenging RF environment.
TR 2.32	The controller shall be highly available with minimum downtime.
TR 2.33	The controller shall ensure seamless roaming.
TR 2.34	The controllers shall communicate back and forth with the Network Management System (NMS) in real time.
TR 2.35	The controller shall have inbuilt wireless intrusion protection capabilities.
TR 2.36	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.
TR 2.37	The controller shall support automatic radio channel adjustment for intelligent channel switching and real-time interference detection.
TR 2.38	The controller shall support user load balancing to balance the number of users across multiple APs to optimize AP and user throughput.
TR 2.39	The controller shall be capable of managing authentication, encryption, VPN connections, IPv4 and IPv6 Layer 3 services.
TR 2.40	The controller shall have redundant power supplies to maintain uninterrupted network operations.
TR 2.41	The controller shall meet the following power specifications: • AC input voltage: 100 VAC to 240 VAC • AC input frequency: 50-60 Hz
TR 2.42	The controller shall support two (2) dual-media ports: 2 x 10 Gigabit Ethernet interface or more.

TR 2.43	The controller shall meet the following environmental specifications: • Operating temperature range: 10°C to 40°C • Operating humidity of 10% to 80% non-condensing
TR 2.44	The Wi-Fi controller shall be reliable ensuring fast, dependable bandwidth and industry standard encryption for security.
TR 2.45	The controller shall be rack mountable.
WI-FI MANAGEMENT SYSTEM	
TR 2.46	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 MCC which will further be integrated to ACC. It shall support plug-and-play environment with zero configuration.
TR 2.47	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.
TR 2.48	Database: The system shall have a centralized database and subscriber management system.
TR 2.49	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.
TR 2.50	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
TR 2.51	The system shall be capable of restricting bandwidth to a user/users as per the policies.
TR 2.52	The system shall be both IPv4 and IPv6 compliant.
TR 2.53	The system shall be capable of logging and creating real time reports for users per access point and controller the bandwidth usage.
TR 2.54	The system shall be capable of displaying a list of managed devices and access points associated to the Wi-Fi controller.
TR 2.55	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.
SERVER	
TR 2.56	The system shall support a centralized servers for user authentication, authorization and accounting.
TR 2.57	The server shall have an integrated embedded management solution to monitor the server for ongoing management, service alerting, reporting and remote management.
TR 2.58	Please refer to the Server Specification as mentioned under IT infrastructure Section 2.2.7.4

2.2.3 City Surveillance with ATCC and ANPR Cameras

2.2.3.1 Overview

Since vision of AURIC is to position it as 'safe' smart city where paramount emphasis is kept on safety of citizens and law enforcement. As part of this vision, IP based video surveillance system shall be implemented across all strategic locations throughout AURIC-Bidkin Phase-1. This shall provide an integrated platform for enabling real-time monitoring and control between multiple departments responsible for safety and security while creating an interactive response management system. These locations comprise of the following as a minimum:

- Roads;
- Intersections/Junctions;
- Entry/Exit points;
- Public spaces/ buildings; and,
- Around critical facilities like Mini Control Centre, Point of Presence (PoP) locations, Solid Waste Management Sites, Bus Stops, Sub-stations, etc.

Depending upon the objective to be served by a camera, they shall be of different configurations. Along with CCTV cameras (Fixed and PTZ), Automatic Traffic Counters and Classifiers (ATCC) and Automatic Number Plate Recognition (ANPR) cameras shall also be installed at all the entry/ exit points of Phase-1 of AURIC-Bidkin. The ATCC shall be capable of automatically counting and classifying all types of vehicles under all lighting and weather conditions. Automatic Number Plate Recognition (ANPR) cameras shall enable functionalities such as number plate detection, information retrieval and storage, analytics etc.

Further, by efficiently leveraging the end-to-end fibre optic network across Phase-1 of AURIC-Bidkin, the MSI shall design and develop entire city surveillance network in a manner so as to ensure minimal points of failure. CCTV surveillance system shall support both edge analytics and central video analytics, ensuring the accomplishment of following objectives:

- Monitor;
- Recognize; and,
- Detect.

To ensure that intelligent surveillance be performed by the CCTV surveillance cameras across Phase-1 of AURIC-Bidkin, the camera equipment shall be housed in a robust housing capable of withstanding extremely adverse weather conditions prominent in the project area. The camera equipment housing shall also ensure that it remains protected from any sort of damage, tampering, theft, vandalism etc.

The MSI shall optimize the network architecture in such a way that the video feeds received from all the cameras shall be directed to AURIC Control Centre for viewing and analytics. However, Mini Control Centre (MCC) shall consist of local server and storage equipment as a minimum for storing all these video feeds. In addition, video feeds shall be available at MCC for viewing purposes. As part of AURIC-Shendra procurement, Shendra MSI has already implemented Honeywell's Digital Video Manager (DVM) R600 at AURIC Control Centre (ACC). Bidkin MSI shall leverage existing DVM and integrate Bidkin's CCTV data. This activity will require scaling up existing DVM in this regard.

2.2.3.2 Architecture

As the CCTVs shall be co-located with other field equipment at the street light poles, the same switch (as used for other equipment) shall be used to backhaul data to the MCC. For connectivity, CCTVs will be connected to the nearest PoP via dedicated Layer-2 industrial grade switch. At the MCC (Primary PoP) location, there will be local storage that will be integrated to the CCTV surveillance system for real-time recording and storage purposes. Further, the MCC shall be integrated with the ACC through a dedicated telecom connectivity.

The real-time interaction and integration with the different ICT systems across the AURIC along with relevant authorities shall result in the overall development of an interactive response management system. Cross-

systems integration of city surveillance system with other smart city ICT elements in real-time shall ease the AITL staff to ensure enhanced and proactive security to both its citizens as well as the industrial workforce of AURIC-Bidkin. Therefore, with such 'smart' surveillance systems being planned for implementation across the Phase-1 of AURIC-Bidkin, the MSI shall ensure efficient, integrated and intelligent operations of the city surveillance system. A brief architecture illustrating the overall operations of city surveillance system has been given in the Exhibit 7 below:

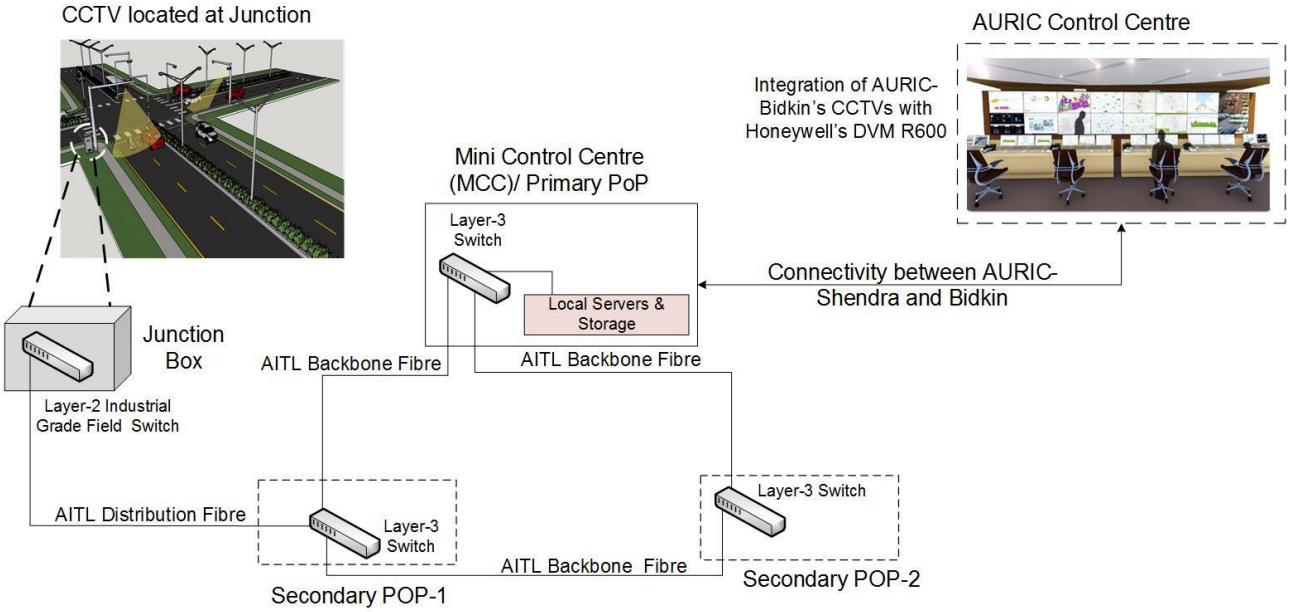


Exhibit 7: Conceptual architecture - City Surveillance System

2.2.3.3 Video Feeds Transmission to AURIC Control Centre

Primarily, the CCTV cameras of Bidkin shall be monitored and controlled from MCC. The video feeds from AURIC-Bidkin Phase-1 shall also be transmitted to AURIC Control Centre (ACC) for viewing at 2CIF resolution (configurable). However, critical alerts shall be enabled as part of this system for 4CIF resolution at ACC.

BR - 3 Business Requirements

BR 3.1	City Surveillance System shall support edge analytics and central analytics for pro-active monitoring.
BR 3.2	ATCC shall include capability to detect, count and classify traffic at all entry and exit locations for the purpose of managing traffic incidents.
BR 3.3	ANPR shall support functionalities such as number plate detection, information retrieval and storage, analytics etc.
BR 3.4	City Surveillance System shall enable real time recording of the video.
BR 3.5	CCTVs shall be co-located with the street light poles along with the Wi-Fi access points and leverage the same switch as the Wi-Fi access points.
BR 3.6	City Surveillance System of AURIC-Bidkin Phase-1 shall be integrated with the Honeywell's DVM R600 located at AURIC Control Centre at Shendra.

FR - 3 Functional Requirements

GENERAL	
FR 3.1	City Surveillance System shall consist of: • Fixed Cameras; • PTZ Cameras; • Automatic Traffic Counter and Classifier (ATCC) with Application; • Automatic Number Plate Recognition (ANPR) with Application; • Local Storage and Servers; • Camera Accessories i.e. Power Supplies, Cable, Connectors and associated accessories for an integrated system.
FR 3.2	The cameras implemented as part of this Project shall be rated for operations in outdoor environment (for outdoor installations) and depending on the objective/application, shall be of different configurations including PTZ or fixed cameras.
FR 3.3	All the Cameras shall be IP based.
FR 3.4	Cameras shall have an integral receiver/driver/ encoder that shall be capable of controlling pan-tilt, zoom and focus locally and also remotely from the ACC.
FR 3.5	Viewing shall also be enabled at the MCC for all the cameras being installed as part of Bidkin Phase-1 Project.
FR 3.6	All the cameras being installed as part of AURIC-Bidkin Phase-1 project shall be integrated with the Honeywell's DVM R600 located at ACC. Video feeds from AURIC – Bidkin Phase-1 shall be transmitted to ACC.
FR 3.7	All cameras shall support real-time video content analysis.
FR 3.8	All CCTV cameras shall be installed on streetlight poles except for multi-services digital kiosks where they shall be integrated.
FR 3.9	Indicative list of capabilities that AURIC-Bidkin city surveillance system are as follows: • Real-time monitoring of City • Event based monitoring of City • Providing secured access to video at any time from any network location • Situation/Rule based alerts including early warnings for prevention and avoidance of unwanted incidents • Automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies

	• Access to historic video data for investigative purposes • Real time traffic counting and classification for managing traffic incidents
AUTOMATIC NUMBER PLATE RECOGNITION (ANPR) SYSTEM	
FR 3.10	The ANPR System recognise the number plates of these vehicles which is then passed on to various other sub-systems for further analytics.
FR 3.11	The ANPR System shall be core to identifying the hot listed vehicles & vehicles for post incident analysis by Police such as security matters, accident detection etc.
FR 3.12	The ANPR system shall capture vehicle license plate from front or from rear depending on the proposed solution and ensuring the performance parameters are met.
FR 3.13	The ANPR sub-system is also used for identifying hot-listed vehicles for ensuring law & order in the city of Bidkin.
FR 3.14	The ANPR sub-system shall be used for satisfying various add-on use- cases such as travel time estimations, estimating O-D patterns in the city, stolen vehicle identification etc.
FR 3.15	ANPR system is used to identify and recognise vehicles by their registered number plates.
FR 3.16	The ANPR shall be deployed at various potential locations across the city of Bidkin Phase-1 viz. entry/exit points, strategic intersections, mid-blocks, sensitive zones etc.
FR 3.17	ANPR system shall capture and read each and every vehicle number plate that passes through its field of view in multiple lanes and stores the number in the database.
FR 3.18	The ANPR system shall continuously record all footage in its field of view which is to be stored at a MCC.
FR 3.19	The ANPR system shall be able to detect and recognize the English alpha numeric License plates in all standard fonts and formats of all vehicle classes irrespective of the type and size of the vehicle.
FR 3.20	Apart from standard printed and High Security license plates, the system shall be able to recognize hand painted straight font alpha numeric number plates in standard formats found on Indian license plates.
FR 3.21	The system processing shall be in real time i.e. the recognition of license plate number should happen instantaneously (within three seconds of capture).
FR 3.22	The system shall be able to process and read number plates of vehicles with speeds up to 150 km/h with the minimum accuracy requirement specified in this sub-section.
FR 3.23	The system shall be very robust to variation in License Plates in terms of font, size, contrast and colour and work with good accuracy but should always be well above the minimum accuracy defined in this sub-section.
FR 3.24	The ANPR shall be able to process and read the number plates at any time of the day and night, in all weather conditions.
FR 3.25	The ANPR sub-system shall have the following minimum accuracy levels irrespective of any other reason at the installed location for each of the vehicles in the field of view during any time of the day or night: • at a minimum of 95% vehicle detection accuracy. • the system should have a conversion accuracy of more than 85% for the detected vehicles for ANPR for standard format license plates. • the system should have a conversion accuracy of more than 75% for the detected vehicles for ANPR for non- standard format license plates.
FR 3.26	The following are the minimum details of the infracting vehicle to be captured: • Location Name and ID along with Latitude and Longitude • Date & Time of the instance • Vehicle Number plate (Captured & Processed) • Image of the vehicle

	• Direction of Travel • Speed of the vehicle
FR 3.27	ANPR system shall be integrated with the RTA and VAHAN database to extract the registered details of the vehicles based on the captured number plate and the details should be stored in a repository including the following details as applicable: • Vehicle Registration Plate Number • Date of Registration • Name of the Person of which the Vehicle is registered to • DOB of the Person of which the vehicle is registered to • Date of Renewal • Location of Issuing Registration Authority Office • Class of Vehicle • Vehicle Colour • Vehicle Insurance No. (historic and Active) • Insurance Validity Date • Vehicle Fitness No. • Fitness Validity Date • Vehicle Permit No. • Permit Validity Date • Load permit • History of Violations
FR 3.28	ANPR shall work with various analytics as defined in this section for identifying and capturing various traffic related incidents & for proposing remedial action.
FR 3.29	The ANPR sub-system shall be able to connect to external sources/ 3rd party databases and check each captured ANPR vehicle numbers against these sources to detect any hot-listed vehicle.
FR 3.30	The ANPR system shall immediately send a configurable high-alert to the pre-designated people with details of the hot-listed vehicle and all other captured details.
FR 3.31	The ANPR system shall automatically send the high alert to the ACC for next course of action.
FR 3.32	The ACC shall internally alert other subsystem to continuously track the vehicle at every junction, notifying the nearest patrolling vehicle and other intercepting teams. ANPR application shall also be used for add on use cases such as travel time estimations, estimating O-D patterns in the city, stolen vehicle identification etc.
FR 3.33	Court Evidence Standard Procedure – The ANPR system should provide the coloured video & image evidences of hot listed vehicles to be submitted in the court.
FR 3.34	The tamper-proof video extract shall be provided as a supporting evidence (for submission in a court of law) to each infracting vehicle and the video length shall be t-5 to t+5 seconds where t being the instant at which the infraction occurred. The video output should be in colour in any industry standard format such as MJPEG, MP4, AVI etc.,) with visually readable license plate number.
FR 3.35	ANPR cameras shall be installed on the gantry along with the ATCC cameras.
AUTOMATIC TRAFFIC COUNTERS & CLASSIFIERS (ATCC) SYSTEM	
FR 3.36	The ATCC system shall be deployed on city road primarily on city's entry and exit points in Bidkin Phase-1. The objective of the sub-system is to collect traffic data at major points. The system shall perform data collection, data storage, file management and report generation functions for collected vehicle information.
FR 3.37	The data from ATCC shall be used by various Government and private organizations (as per AITL discretion) to understand the existing traffic volume trends & patterns.
FR 3.38	The real-time traffic data can be shared with 3rd party map solution providers and online navigation systems as per the discretion of AITL.

FR 3.39	The ATCC Sub-system shall support the following four use-cases with other Sub-systems provided by 3rd parties as a minimum and shall support development and deployment of any other use-case for up to 18 months from the Go-Live date. • Use case 1: Passing Congestion Information to ACC and MCC. • Use case 2: Using Traffic Data Archive for future planning/ Design/ Analysis purposes.
FR 3.40	The ATCC System shall use any proven non-intrusive technology for counting and classifying the vehicles in a real-time under live traffic conditions.
FR 3.41	The field view of ATCC on a road stretch shall be able to cover from end to end of the traffic lane irrespective of the number of lanes on the particular road stretch.
FR 3.42	The number of ATCC sensors required to achieve a multi-lane road stretch shall be arrived by the MSI based on the physical surveys of site and technology being provided and other criteria.
FR 3.43	The ATCC System at any point of time, shall provide a minimum of 5 classification levels viz. 2-wheeler, 3 Wheeler/Auto Rickshaws, Car/ Jeep, LCV, Bus/Truck/MAV at any given point in time.
FR 3.44	The ATCC system shall meet the following accuracy levels when compared with actual data collected using other means at each location of all the installed locations (minimum accuracy requirements): • Counting of vehicles: > 95% • Classification of vehicles (w.r.t. each class): > 90%
FR 3.45	System shall insert sequence numbers for vehicle records.
FR 3.46	The ATCC shall have built in algorithms to distinguish and classify non- linear traffic patterns and occlusion of traffic.
FR 3.47	ATCC sensors shall capture the traffic data 24x7 lane wise, leg wise and transfer the traffic data to MCC and ACC through fibre backbone in real time.
FR 3.48	There shall be an operator at ACC/MCC to operate the ATCC application on ATCC workstation.
FR 3.49	The data of ATCC shall also be available in open data source which can further be used in other applications.
FR 3.50	The overall system shall work in an integrated fashion whereby data from the ATCC shall be continuously recorded, processed and transferred to MCC and ACC.
FR 3.51	The algorithm (software) shall be capable of adding configuration parameters for each of the vehicle classes based on the RTA standards and field conditions to achieve maximum accuracy
FR 3.52	ATCC shall be able to process simultaneous and parallel passages of the vehicles at that location at a given point of time.
FR 3.53	Even though multiple sensors are required based on the number of actual lanes, the ATCC should provide processed data at each location lane wise and leg wise.
FR 3.54	The ATCC shall count and classify vehicles travelling in any or both the directions at a given location as per the requirement based on the field conditions.
FR 3.55	The ATCC shall be able to count and classify the vehicles with minimum accuracy requirements for vehicles travelling between 10 kmph to 150 kmph speeds.
FR 3.56	The ATCC sub-system should be capable of capturing at a minimum the following primary data points for each vehicle at any point of time: • Unique ID • Vehicle Count • Start Time • End Time • Leg/ road Location • Classification • Headway

	• Occupancy • Vehicle Length • Speed
FR 3.57	The ATCC sub-system shall be capable of computing unlimited Derived fields/ data sets based on several mathematical computations on the primary data points collected. In general all computations required for deriving several Traffic Engineering measures shall be supported by the ATCC reporting module.
FR 3.58	The ATCC sub-system provider shall work closely with client for modifying/ configuring standard existing reports and data formats to suit client requirements. The vendor shall support client in developing any/ all reports and formats required by the agency for a period of at least 18 months from the system go-live date.
FR 3.59	The ATCC Sub-system shall be capable of sharing the data with any other sub-system in a real-time as per the requirement
FR 3.60	The ATCC provider shall work closely with various other sub-system providers to share the required data in acceptable format to the other sub- system providers. As a minimum data exchange in XML, HTML and JSON formats shall be supported
FR 3.61	The ATCC system shall have an operations monitoring dashboard, located at the ACC/MCC & shall be monitored by the operator.
FR 3.62	On this dashboard there shall be a schematic layout of the ATCC showing all the connected nodes on the GUI.
FR 3.63	The various nodes when connected & disconnected shall be represented in different colour schema on the GUI of the ACC/MCC operator.
FR 3.64	If any particular node is disconnected from the control room, the same shall raise an alarm to the ACC operator GUI & appropriate action shall be taken to rectify the same.
FR 3.65	The monitoring dashboard shall allow the ACC/MCC operator to click on any node & view the details of “operator” logged in, time duration since logged in, summary of operations performed, disable/enable ATCC.
FR 3.66	If operator or any other user from ACC/MCC disable/enable/operate any active device remotely, the same shall be captured in Control Centre activity report with all details including but not limited to date, time, device, action performed etc.
FR 3.67	The monitoring dashboard shall show the status (connected/disconnected, faulty/working) of all logical devices (ATCC system) connected to a particular node when clicking on a node from the monitoring dashboard GUI.
FR 3.68	In case of any fault in the devices connected to a node, or connectivity failure with a node, a pop-up message shall appear on the monitoring dashboard workstation. The operator has to acknowledge the pop-up message & report the type of fault to the maintenance team & shall record the details to the assigned team/individual into the system.
FR 3.69	Fault assignment to the maintenance team shall be managed and controlled by the system software only. Once a fault is assigned by the ACC/MCC operator or authorized user to the maintenance team, the same shall be displayed in the maintenance module and once fault is closed/resolved by the maintenance team it shall be updated automatically (in case of active devices) or else updated manually in the software application/maintenance module.
FR 3.70	The access to monitoring dashboard shall be specific to the privilege of the user which can be defined in the system & shall be specific to a group/part of node locations.
FR 3.71	ATCC system shall be installed on the gantry along with the ANPR cameras.
FR 3.72	ATCC Controller or Local Processing Unit shall have capability to store at least 1 month data for field level.
FR 3.73	The field equipment including the sensor shall be capable of operating independent of other layers. This is to say that the sensor shall be capable of storing the data as well as event messages locally

	irrespective of the status of the communication link for a defined period (1 month). Whenever the communication link is restored, the offline data shall be sent to the ACC/MCC automatically. However, it shall be possible to transfer the data manually by copying the same from the DL to a thumb drive / lap top and restoring the same into the control centre database. As soon as the link is restored, the locally stored entries which were not transferred due to link failure shall automatically be sent to control centre and a mechanism shall be used to ignore duplicate entries of manually transferred data at control centre level.
FR 3.74	There shall be no double count in case of lane crossover / straddling. Anti-coincidence technique shall be used to avoid such incidents of single vehicle activating two or more lane sensors. It shall however send the raw data as well as the processed information, wherever anti-coincidence in utilized.
FR 3.75	The vehicle count shall not be missed even when multiple vehicles cross different lanes at simultaneous instances.
FR 3.76	ATCC Controller or Local Processing Unit shall be vandal or tampering proof.
CAMERAS WITH BUILT-IN VIDEO ANALYTICS	
FR 3.77	The surveillance system shall support following Built-in-Analytics for the Cameras and using central analytics: • Auto Tracker: To detect and track movement in the field of view. • Adaptive Motion Detection: To detect and track object that enter a scene and then triggers an alarm when the object enter a user-defined zone. • Abandoned Object: To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows. • Camera Sabotage: Triggers an alarm if the lens is obstructed. • Directional Motion: Generates an alarm in a high traffic area when a person or object moves in a specified direction. • Object Counting: To count the number of objects that enter a defined zone. • Object Removal: To triggers an alarm if the object is removed from a user-defined zone. • Stopped Vehicle: To detect vehicles stopped near a sensitive area longer than the user-defined time allows. • Intrusion Detection: Detect intrusion.
FR 3.78	Event (alarm) Handling: • The camera shall be capable of recording an event as pre and post event images. Events may be triggered using camera motion detection or from an external device input such as a relay. • When triggered from an external input or the camera's motion detector, the camera shall be capable of sending JPEG images via e-mail and/or sequences of images to local servers and storage. • A relay output shall be available upon the activation of the camera's motion detector or external relay input. The relay output may also be manually activated from the live view screen.
STORAGE SOLUTION	
FR 3.79	Storage Solution at MCC shall have in-built capabilities of recording video streams directly from IP based cameras installed at field.
FR 3.80	Storage for video feeds should not have any single point of failure. It shall have self-healing design that should protect against disk or node failure including storage backend failover.
FR 3.81	The overall storage solution shall scalable up to two (2) times of current usable disk space storage without addition of controllers.
FR 3.82	The storage solution proposed is that the video feeds would be available for minimum 30 days. After 30 days, the video feeds can be overwritten or archived unless it is flagged or marked by the Police or AITL for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police or AITL deem it good for deletion.

FR 3.83	For incidents that are flagged by the Police, AITL or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted.
FR 3.84	The Recording Servers/Storage, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.
FR 3.85	The system should not limit amount of storage to be allocated for each connected device.
FR 3.86	The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
FR 3.87	The Recording Servers/Storage, shall support camera devices from various OEMs.
FR 3.88	The storage system shall support all latest versions of Windows, Linux, and UNIX.
FR 3.89	The storage software shall be web-accessible GUI Configuration and shall support the management with online upgrades.
FR 3.90	The system shall have a dedicated purpose build Storage Operating System and hardware shall be required to meet the desired functionality in scale-out storage architecture.
FR 3.91	The storage solution should include 1 host spare for every 30 drives.
VIDEO MANAGEMENT SYSTEM (VMS)	
FR 3.92	All the CCTVs installed at AURIC-Bidkin Phase-1 shall be integrated with the Honeywell's Digital Video Manager (DVM) R600 being installed at AURIC Control Centre (ACC) located at Shendra.

TR - 3 Technical Requirements

FIXED & PTZ CAMERA, LENSES AND MOUNTS	
TR 3.1	The camera control shall comply with the latest release of Open Network Video Interface Forum (ONVIF) standards.
TR 3.2	The camera shall include an integral receiver/driver/ encoder. The receiver/driver shall be capable of controlling pan-tilt, zoom and focus locally and remotely from the MCC and ACC.
TR 3.3	The camera shall incorporate AGC circuitry to provide for compensation at low light levels.
TR 3.4	The lens shall be integrated with the camera.
TR 3.5	Video output resolution shall be as per respective camera lens specifications.
TR 3.6	The camera shall be capable to produce minimum 15 frames per second (fps).
TR 3.7	The camera shall provide automatic white balance, automatic exposure, automatic gain control, electronic shutter, and backlight compensation.
TR 3.8	The camera shall be a true day/night cameras with mechanical IR cut filter.
TR 3.9	The camera shall be capable of providing a high contrast colour picture with a full video output at a minimum illumination as mentioned in the specifications.
TR 3.10	All cameras shall capture high definition video, compress the video using H.264 or better technique and transmit real-time using fibre optic based communications system.
TR 3.11	The cameras shall capture audio and compress using G.711 technique and transmit real-time using fibre optic based communications system.
TR 3.12	All cameras shall support on-board real-time video content analysis.
TR 3.13	All cameras shall support both Constant Bit-Rate (CBR) and Variable Bit-Rate (VBR) options.

TR 3.14	The camera shall support up to 2 video profiles as a minimum, each providing independent configuration of bitrate, frame rate and resolution.
TR 3.15	The camera shall support on-board storage via micro SDHC slot and card with a minimum capacity of 32 GB.
TR 3.16	All cameras shall have integral in-built adaptive IR technology. For fixed cameras, the IR shall support a range of at least 60 m and for PTZ it shall support a range of at least 100m moving with zoom (adaptive).
TR 3.17	For Fixed Cameras: • The fixed camera shall provide a minimum focal length range of 2.8-10 mm or better compensated with a minimum 12x digital zoom and shall be remotely controllable from the camera control transmitter at Primary Control Centre. • The fixed camera shall capture video using 1/3" progressive scan CMOS or better. • Fixed Camera resolution shall be 3 Megapixels or better.
TR 3.18	For PTZ Cameras: • Camera shall have capabilities of PAN of 360° continuous. • Camera shall have capabilities of Tilt of 90 deg. with Auto Flip. • Lens of 6mm-129mm with minimum 30X optical and 12X digital zoom. • PTZ camera shall capture video using minimum 1/3" type CMOS sensor or better. • It shall support resolution of 2 Megapixels or better. • Camera shall support tilt of 100° either side. The tilt capability shall include both the horizontal (level view) and vertical (downward view) position. If the camera travels beyond straight down, automatic image flip circuitry shall prevent the display of an inverted image. • The pan and tilt mechanism shall be an integral part of the camera. • Pan speed shall be up to 160°/s and Tilt speed up to 100°/ sec.
TR 3.19	There shall be a minimum of 100 assignable automatic preset positions.
TR 3.20	There shall be 4 or more definable privacy zones as per project requirements.
TR 3.21	All cameras shall provide effective 24/7 imaging performance for CCTV surveillance applications.
TR 3.22	All cameras shall provide user control, with remote configuration for functions including streaming and compression settings, exposure, white balance, flicker control, picture size, cropping/privacy, brightness, sharpness, saturation, day-night switching point, frame rate, image rotation, snapshot, dynamic bandwidth allocation and motion detection.
STORAGE SOLUTION	
TR 3.23	The storage solution shall be supplied with at least four (4) nos. of 10G IP Ports.
TR 3.24	Bandwidth optimization - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG-4, etc.) and frame rate (4CIF or better) options for managing the bandwidth utilization for live viewing at ACC.
TR 3.25	The storage system solution shall ensure a minimum total aggregate of 1200 Mbps configuration; 90% sequential write & 10% sequential read application environment.
TR 3.26	MSI shall also provide minimum 50 TB usable Storage capacity based on RAID 6 or equivalent at MCC using SSD/Flash drives for virtual infrastructure. The capacity shall be provisioned with FC protocols for host access with efficiency features i.e. compression and deduplication.
TR 3.27	The storage array shall be calculated by MSI with best quality cameras (minimum 20 fps, at H.264 compression) with minimum storage & Bandwidth with best video quality using minimum 7200 rpm or better drives protected by RAID 6 or equivalent.

TR 3.28	The solution shall sustain failure of minimum 2 drives for every 20 data drives supplied.
TR 3.29	The solution shall include 1 host spare for every 30 drives.
AUTOMATIC TRAFFIC COUNTER & CLASSIFER (ATCC)	
TR 3.30	The Automatic Traffic Counter and Classifier System (ATCC) shall have the capability of vehicle presence detection & classification at free flow roads.
TRAFFIC DATA COLLECTION	
TR 3.31	The system shall also be cost effective solution for traffic data collection and traffic flow monitoring on highways and inter-urban roads.
TR 3.32	It shall be used for temporary or permanent application both.
TR 3.33	There shall be single download tool to download the integrated traffic data and traffic events from multiple sensors.
TR 3.34	The system shall have the facility to monitor the traffic data, events and viewing maps through the graphical user interface, it is possible to create maps in order to have an overview of all installed sensor systems. By double clicking on a camera, to get live streaming video from the selected sensor. There shall be an event stack which can groups all the traffic data & traffic events.
TR 3.35	The system shall have the capability to capture vehicle count (per lane and per vehicle class).
TR 3.36	The system shall have the capability to capture vehicle speed (per lane and per vehicle class).
TR 3.37	The system shall have the capability to capture vehicle occupancy (per lane).
TR 3.38	The system shall have the capability to capture vehicle Headway (per lane).
TR 3.39	The system shall have the capability to capture vehicle different classification (two wheeler, three wheeler, car, bus, trucks etc.).
SENSOR SYSTEM COMPONENTS	
TR 3.40	The system shall cover up to minimum 4 lanes.
TR 3.41	The system shall have the capability to connect minimum 4 sensor at a time.
TR 3.42	The electronic shall be din rail mountable and shall have the lock and key facility.
TR 3.43	The system shall have the following features: • Controller area network bus design for option to add sensor interface boards. • On-board Ethernet interface • RS-232 interface • Remote administration via Telnet or web based program • Remote file download
TR 3.44	The system shall have the capability to connect with local computer using a password protection system.
TR 3.45	The local computer software shall have the compatibility of system configuration, viewing, recording, data collecting & monitoring.
TR 3.46	System shall have non-volatile local storage for vehicle information to prevent data loss during power outages.
TR 3.47	System components shall contain necessary electrical protection to prevent damage from electrical surges, spikes and the effects of lightning.
GENERAL FOR SURVEILLANCE SYSTEMS	
TR 3.48	All CCTV cameras shall support Power over Ethernet (PoE and PoE+).

TR 3.49	ATCC system shall preferably support PoE or PoE+. Alternatively, ATCC system shall support 24VAC/24VDC or 230 VAC operation.
TR 3.50	The camera shall use an Ethernet 10/100Base-TX network interface with RJ45 connector.
TR 3.51	The camera and the associated equipment shall support communication protocols IPv4, IPv6, TCP, UDP, HTTP, HTTPS, DHCP, IGMP, ICMP, SNMP, FTP, NTP, RTSP, and RTP as a minimum.
TR 3.52	The camera shall incorporate a built-in web server, built-in FTP server, and a built-in FTP client.
TR 3.53	The cameras shall have, at a minimum, the following configurable features: • Image resolution • Frame rate • Image quality adjustments (brightness and contrast) • Source and destination IP address settings • UDP port number • Bandwidth limits • Unicast and multicast settings and support for two (2) simultaneous unicast streams.
TR 3.54	The cameras shall support at the minimum three individually configured video streams. The cameras shall be capable of three or more simultaneous streams with one of the streams being in H.264 or better format.
TR 3.55	All cameras shall have an operating temperature range of 0°C to +55°C at humidity: 5% - 95% RH.
TR 3.56	The environmental housing shall be of suitable size and provide a temperature controlled atmosphere for the camera, lens and receiver-driver/ encoder.
TR 3.57	The housing shall allow for easy disconnect of all external cables.
TR 3.58	The housing, mounting arm and the dome camera installed assembly shall be suited to withstand wind gusts of 150 km/h.
TR 3.59	The housing for CCTV shall meet the IP66 for protection.
TR 3.60	The cameras shall have a Mean Time Between Failure (MTBF) of at least 100,000 hours.

2.2.4 Multi-Services Digital Kiosk

2.2.4.1 Overview

Multi-Services Digital Kiosks will be deployed across AURIC-Bidkin Phase-1 to give the citizens access to various services via one integrated platform. This will be a dedicated and fixed structure which will include Wi-Fi access point, emergency call button, charging points, solar panels, access to citizen services including capabilities to make payments for citizen services and bills using touch screen, static advertising on up to three (3) faces, Smart Card Reader and CCTV. Multi Services Digital Kiosks shall be installed at strategic locations such as AITL buildings, public parks, Exhibition Pavilion, etc.

2.2.4.2 Architecture

Multi-Services Digital Kiosk shall be connected with the MCC using the fibre optic infrastructure. Kiosk's data shall further be transmitted to ACC at Shendra for operations through the dedicated connection between MCC and ACC. A switch shall be housed inside each multi-services digital kiosk from where the data will be backhauled to the nearest PoP over the fibre optic infrastructure. A conceptual architecture for the same has been presented in Exhibit 8 below.

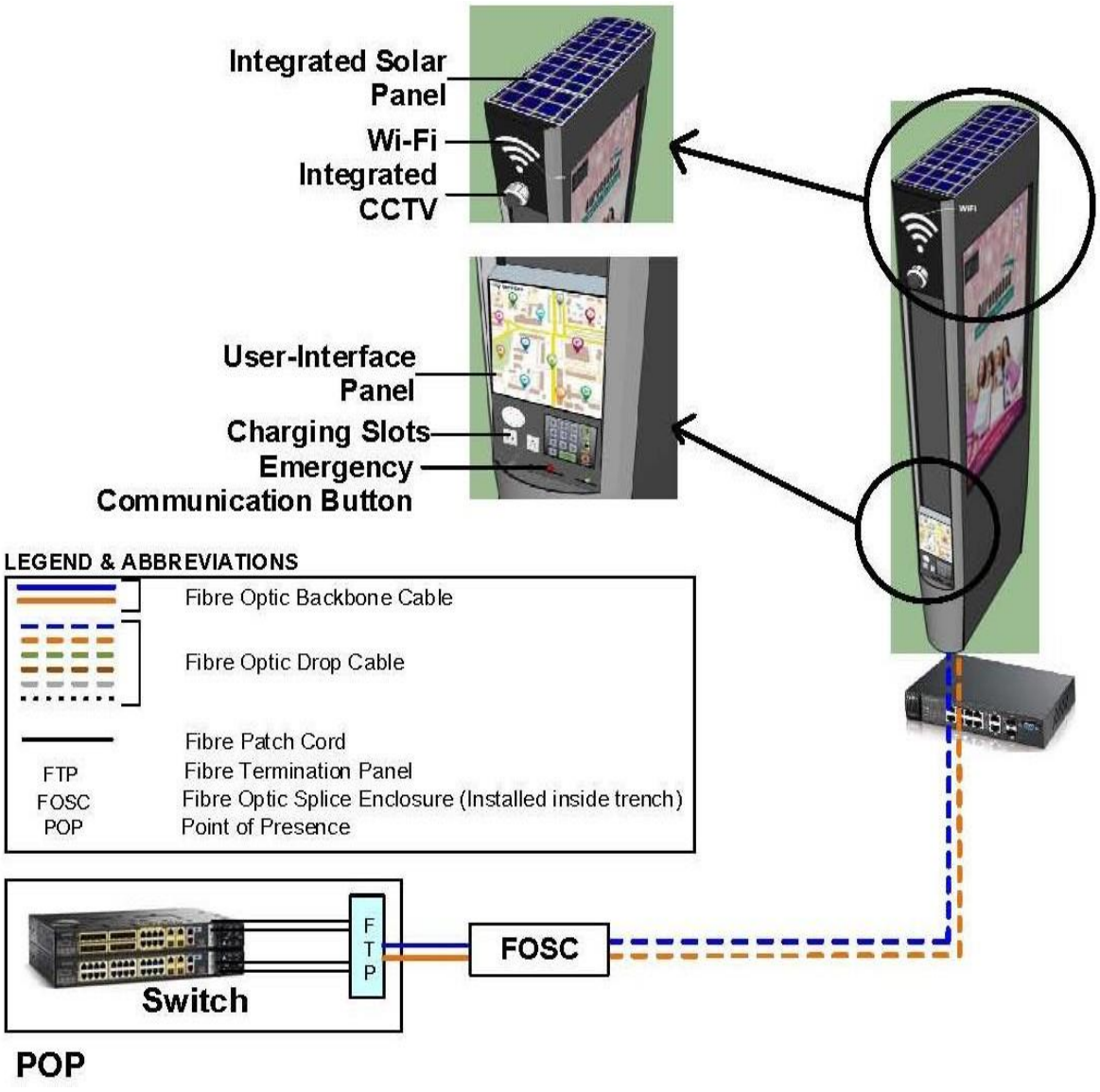


Exhibit 8: Conceptual architecture for Multi-Services Digital Kiosk

BR - 4 Business Requirements

BR 4.1	Multi-Services Digital Kiosk shall provide various services and information to citizens, visitors, as well as AITL staff, integrated using one common platform.
BR 4.2	Multi-Services Digital Kiosk shall also be the contact point for citizens who are not connected to smart phones or e-mail.
BR 4.3	Multi-Services Digital Kiosk shall be deployed at strategic locations such as Bus Stops, Exhibitions Pavilion, AURIC or other government associated buildings, hotels, malls etc.
BR 4.4	Using the Multi-Services Digital Kiosk, citizens shall be able to avail multiple city services integrated via the e-governance platform plus shall provide the capability for bill payments.
BR 4.5	Multi-Services Digital Kiosk shall include the following in one integrated structure – emergency call button, touch screen for citizen services with payment options (integrated with e-wallets, debit and credit card), smart card reader for smart card (with additional security features such as PIN), integrated CCTV, Wi-Fi and Solar Panel with batteries, plus additional space for static advertising/promotions.
BR 4.6	Multi-Services Digital Kiosk shall also include capabilities for providing services to differently abled users. As one example, height of ECB shall be such that it supports usage for a person on wheelchair. Bidder to propose other possible scenarios.
BR 4.7	Multi-Services Digital Kiosk shall integrate with MCC and ACC for centralized operations.

FR - 4 Functional Requirements

FR 4.1	Multi Services Digital Kiosk shall have integrated: • Emergency Call Box (ECB) • CCTV • Wi-Fi access point • Common payment card (Smart Card) • Ability to pay bills using e-wallet, debit card and credit card. • Touch screen for availing citizen services with in-built interactive platform • Integration with environmental sensors to display information from various sensors • Solar panel with batteries • Charging slots • Static advertisement on up to three faces • Microphone • Speaker • Keypad for entry of pin for authentication • Smart card reader • Printing of any receipts All these components shall be supplied as part of the integrated Multi Services Digital Kiosk.
FR 4.2	Multi-Services Digital Kiosk's power requirements shall be met by an integrated solar panel as primary source of power (with runtime of 8 hours) with support of raw power for backup purposes. The solar panel batteries shall be installed within the housing of the kiosk in an integrated manner.
FR 4.3	Multi-Services Digital Kiosk shall be fixed units, embedded inside the ground that shall be weatherproof. IP 65 rated, and rated for performance for outdoor technology street furniture.

FR 4.4	Multi-Services Digital Kiosk enclosure shall have the space to house all the hardware equipment required for the Multi-Services Digital Kiosk including switches, solar panel, batteries, printer for receipts and other associated accessories. All the wiring shall be concealed within the Multi-Services Digital Kiosk enclosure and shall not be visible from outside.
FR 4.5	The Emergency Call Button (ECB) shall have the capability to trigger emergency communications with ACC. As the Emergency Call Button is pressed, the call should land up to the operators at the ACC from where it may be routed to the concerned department. MCC operators shall also be enabled to respond to emergency calls.
FR 4.6	The ACC and MCC operators shall able to monitor the video of the user who triggered the ECB. Automatic video recording shall be enabled when ECB button is pressed at multi-services digital kiosks.
FR 4.7	Multi-Services Digital Kiosk shall have in-built speakers and microphone for making an emergency call to/from the ACC and MCC and a keypad for accepting user input.
FR 4.8	The integrated CCTV shall have the capability of recognition. Operators at the MCC and ACC shall be able to monitor the live feed from the CCTV. When the emergency button is pressed, the camera shall automatically focus on the person using the button with a video feed on the video wall at the MCC and ACC. Primary control of the PTZ camera in such an event shall be with the operators at ACC.
FR 4.9	The Multi-Services Digital Kiosk shall have in-built charging slots, i.e. two (2) USB ports and one (1) three pin standard plug port.
FR 4.10	The user-interface panel shall built-in capacitive touch screen for interactive purposes including but not limited to: • Maps and navigation services i.e. displaying routes across Bidkin. • Displaying of bus routes across Bidkin. • Information about Bidkin along with e- governance services. • Environmental related information via integration with environmental sensors. • Places of attraction in Bidkin. • Places near me services which may include hotels, government offices, shops, tourist attraction, etc. • Information about the events. • Emergency contact numbers such as hospitals, police, fire, etc. • Integration with e-governance system. • Integration with digital wallets, credit and debit cards for payments. • Integration with Smart Card. Capability for supporting payments via smart card shall also be facilitated. The Smart Card will be issued by banks and shall be accepted at Multi-Services Digital Kiosks.
FR 4.11	Multi-Services Digital Kiosk shall have a capabilities for making digital payments for: • Utility Bills for government services such as electricity, water, Wi-Fi, etc. • Citizen services • Tickets for the events around the city • Any other AITL supported activity/event
FR 4.12	Multi-Services Digital Kiosk shall have in-built receipt/ticket printer having the functionality of printing of receipts, any other tickets, etc.
FR 4.13	The Multi-Services Digital Kiosk shall have the space for providing the static advertisement around up to three (3) faces.

FR 4.14	The Multi-Services Digital Kiosk shall be multilingual i.e. it shall support languages such as English, Hindi and Marathi.
FR 4.15	The Multi-Services Digital Kiosk shall have ECB and touch panel at an average height of 1.5m above ground.
FR 4.16	Multi-Services Digital Kiosk shall be upgradable through a central system remotely over internet.
FR 4.17	It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network.

TR - 4 Technical Requirements

MULTI-SERVICES DIGITAL KIOSKS	
TR 4.1	Multi-Services Digital Kiosk's enclosure shall be made of metal or stainless steel fabric and shall be IP 65 rated. It shall be built to last in outdoor environment to support the Project operating conditions. Design of the kiosk shall be as per Bidder's solution (for example, kiosk under a cabin etc.) and shall meet the requirements of the RFQ cum RFP.
TR 4.2	Metal sheet of the Multi-Services Digital Kiosk housing shall be made in a minimum 16 gauge that can be powder coated as per the required colour choice.
TR 4.3	Multi-Services Digital Kiosk's enclosure shall have space to put all the required hardware including switches and associated accessories.
TR 4.4	Multi-Services Digital Kiosk's shall have PTZ Camera mounted on the top of the Kiosk Enclosure. For PTZ Camera Specifications, Please refer to the City Surveillance System Section 2.2.3.
TR 4.5	The Camera shall be automatically focused towards the citizen upon pressing of ECB button and shall focus on the user who activated the ECB call with a video feed display at the video wall at MCC & ACC. The ECB call can only be disconnected from MCC or ACC level.
TR 4.6	The control centre operator shall able to monitor the video of the user who triggered the ECB.
TR 4.7	Multi-Services Digital Kiosk shall also have integrated Wi-Fi access points. For Wi-Fi Access Point Specifications, Please refer to the Public Wi-Fi Section 2.2.2
TR 4.8	The Multi-Services Digital Kiosk shall also have integrated solar panel with batteries.
TR 4.9	The Multi-Services Digital Kiosk shall have the capability of integrated payment through which citizens can make digital payment of city services like payment of bills, booking of event tickets, take receipt print of payments etc.
TR 4.10	The Multi-Services Digital Kiosk enclosure shall have integrated receipt printer for taking printout of bills payments receipt and events tickets etc.
TR 4.11	The Multi-Services Digital Kiosk shall have in-built speakers and microphone. Speakers shall be able to deliver clear stereo sound. Microphone shall be able to isolate the main sound source and minimize background noise. At any time, the speakers shall have an output audio of at least 10 dB above ambient noise.
TR 4.12	Multi-Services Digital Kiosk shall have proper ventilation arrangement for heat removal.
TR 4.13	Multi-Services Digital Kiosk shall have proper in-built wiring arrangement with spike proof power socket.
TR 4.14	Multi-Services Digital Kiosk shall have two (2) service doors with security key so that it can be easily accessed from there.
TR 4.15	Multi-Services Digital Kiosk shall be either fixed to ground or have shoes to hold it on a smooth surface.

TR 4.16	All electrical components shall have quick-disconnect terminals for easy service or removal. All wiring shall be concealed within the Multi-Services Digital Kiosk enclosure and shall not be visible from the outside of the unit.
TR 4.17	Multi-Services Digital Kiosk shall be equipped with sufficient tamper-proof mechanisms to ensure detection at MCC & ACC in case of physical tampering to the Kiosk.
TR 4.18	Multi-Services Digital Kiosk shall be upgradable through a central system remotely over internet.
TR 4.19	It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network.
INTERACTIVE USER PANEL FOR INFORMATION OF CITY SERVICES	
TR 4.20	The panel shall have built-in capacitive touchscreen for interactive applications with required supporting software for dynamic content management from various sources connected to the system. The content management system shall include content from (but not limited to) – e-governance platform, services billing, AITL organized/supported events, data from environmental sensors, digital advertising and promotions (provided as part of the content management system), city news and information, among others. Content shall be on the same display and content for kiosk shall be finalized with successful Bidder.
TR 4.21	The touch screen shall be all-glass with a transparent metallic conductive coating. OR with laminated and tempered glass (3.5 mm + 3.5 mm).
TR 4.22	The touch screen monitor shall have a min. resolution of 1280 x 1024 or better with screen size of minimum 24”.
TR 4.23	The screen shall support wide viewing angle, low power consumption, high contrast ratio, high aperture ratio, short response time.
TR 4.24	The content displayed on the panel shall be direct sunlight readable and shall support the feature of auto brightness control.
TR 4.25	The touch screen shall have the embedded thin client with quad core CPU 8GB memory, 32 GB Flash, 1 TB of secondary storage for local storage with required OS.
TR 4.26	The touch screen monitor shall be capable of withstanding most surface contaminants and must be ASTM-D-1308-02 and ASTM-F-1598-95 compliant.
TR 4.27	The touch screen monitor shall be NEMA 4X (IP66) rated and complete water- resistant seal compatible. It shall be capable of operating in outdoor rated environments and shall have a rugged screen.
EMERGENCY CALL BOX	
TR 4.28	The ECB shall be integrated with the Multi-Services Digital Kiosk and shall be monitored at ACC. ECB shall also be integrated with MCC.
TR 4.29	At MCC & ACC, graphical display of the locations of the ECBs mounted on the multi- services digital kiosk shall be provided at the workstations to control, configure and manage ECBs at a minimum.
TR 4.30	The ECB shall be auto-dial operation and shall be capable of automatically answering incoming calls.
TR 4.31	The ECB shall communicate over 10/100/1000 Base-TX copper signal ports over Ethernet.
TR 4.32	The ECB shall support SIP based Voice over Internet Protocol (VoIP) communications standard.
TR 4.33	The ECB shall have network connectivity for monitoring via Web access (HTTP), SNMP, and shall provide the capability of e-mail notification of alarm conditions. Multiple alarms of the conditions shall be provided automatically.
TR 4.34	The ECB shall have automatic adjustment of output volume of audio based on ambient noise detection. At any given time, the sound output from ECB speaker shall be 6-10 dB above ambient noise.

TR 4.35	The call from ECB shall only be disconnected at MCC & ACC. The user shall not have the capability to disconnect the call from the ECB itself.
TR 4.36	The ECB button shall be circular, red in colour and the panel shall have clear label of 'Emergency Call Button'.
DIGITAL PAYMENTS	
TR 4.37	The Multi-Services Digital Kiosk shall have the capability for digital payments like electricity bills, water bills, Wi-Fi recharge/coupon, Payment of penalties (Challans, etc.), payment for any city supported events, etc.
TR 4.38	The Multi-Services Digital Kiosk shall accept all digital payments including credit card, debit card and e-wallets.
TR 4.39	The Multi-Services Digital Kiosk shall have option for taking printout of bills payments receipt and events tickets etc. through integrated receipt printer.
TR 4.40	The digital payments for Multi-Services Digital Kiosk shall comply with all the revenue/financial departments' norms and conditions for such online financial transactions in India and shall adhered to all such norms and conditions.
TR 4.41	The Multi-Services Digital Kiosk shall have the capability to integrate with Smart Card which shall be used for making payments at multiple merchandises across Bidkin. The Smart Card shall be issued by Banks and will be accepted at most of the facilities in Bidkin. The Bidder shall work in close coordination with the Smart Card Agency and other related agencies.
SMART CARD READER	
TR 4.42	Multi-services digital kiosk shall have the capability of reading citizen specific smart card as an identity check for availing services.
TR 4.43	Multi-services digital kiosk shall be able to read the smart card from mobile phones, tablets and paper prints.
TR 4.44	The smart card reader shall be supported by a second level of authentication i.e. OTP via SMS at user registered number or similar that shall be inserted by the user using the keypad at the kiosk. Workflows for the same will be finalized during detailed design stage.
ELECTRICAL	
TR 4.45	The Multi-Services Digital Kiosk shall be powered by 12/24/48VDC input as per the design requirements to support powering using solar as the primary power. Raw power will be provided for secondary power. The ECB inside the multi-services digital kiosk shall be powered using PoE or PoE+. 230VAC can also be acceptable however, the Bidder shall provide any power conversion if required to meet the requirements of the RFQ cum RFP.
TR 4.46	The Multi-Services Digital Kiosk shall communicate over RJ45, HDMI/DVI and USB.
TR 4.47	The Multi-Services Digital Kiosk shall support operating temperature range of 0°C to +60°C with ambient relative humidity of 10-95% non-condensing.
TR 4.48	The ECB shall have a MTBF of at least 100,000 hours.
TR 4.49	The touch screen monitor shall have a MTBF of at least 50,000 hours.

2.2.5 Environmental Sensor

2.2.5.1 Overview

Environmental parameters, specifically air and noise pollution, are a major concern for the citizens and administrators of any city. As Bidkin aspires to also be an environmentally sustainable smart city, integrated environmental monitoring stations comprising of various sensors shall be implemented in AURIC-Bidkin Phase-1. The objectives of the system include:

- Integrated ambient air and noise pollution monitoring stations comprising of various environmental sensors for monitoring and trending of various ambient air and noise parameters;
- Tracking of Bidkin's contribution to environment with respect to these parameters and adjusting any framework for the city;
- Environmental sensors shall be integrated with ACC and MCC for central monitoring and analysis;
- Environmental sensor parameters shall be available through City Portal and Applications for citizens as part of 'open data' initiative and to create citizen awareness.

BR - 5 Business Requirements

BR 5.1	Integrated ambient air and noise pollution monitoring stations comprising of various environmental sensors shall be implemented in Bidkin for monitoring and trending of various ambient air and noise parameters.
BR 5.2	Environment monitoring shall be done for tracking that the pollution and noise levels are within the acceptable limits.
BR 5.3	Display of parameters to citizens to create awareness and support 'open data' initiatives.
BR 5.4	Establish frameworks for regulating these parameters in terms of any supporting initiatives for maintaining acceptable levels.
BR 5.5	The existing Environmental Sensor Management Software is of PAQS make. It is required to integrate Bidkin Environmental Sensors with the existing PAQS software.
BR 5.6	Central monitoring at ACC, MCC, city application, website and digital display screen in an integrated manner.

FR - 5 Functional Requirements

FR 5.1	Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station: • Carbon Monoxide (CO) sensor • Ozone (O_3) sensor • Nitrogen Dioxide (NO_2) sensor • Sulfur Dioxide (SO_2) sensor • Carbon Dioxide (CO_2) sensor • Particulate Matter (PM_{10} and $PM_{2.5}$) sensor • Temperature sensor • Relative Humidity sensor • Wind Speed sensor • Wind Direction sensor

	• Rainfall sensor • Barometric Pressure sensor; and • Noise sensor.
FR 5.2	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air and noise quality among other parameters as detailed in point above.
FR 5.3	Environmental sensor station shall be ruggedized enough to be deployed in open air areas such as streets and parks.
FR 5.4	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod stand or a standalone pole.
FR 5.5	The Response time of the sensors shall be less than 60 seconds.
DIGITAL DISPLAY SCREEN (DDS)	
FR 5.6	DDS will be installed at identified strategic location and will be used for display environmental parameters along with other promotional messages. The integrated DDS software application will allow user to publish specific messages & general informative messages.
FR 5.7	DDS shall be integrated with the environmental station for automatically displaying information from environmental sensors.
FR 5.8	A DDS software system shall be provided to the MCC and ACC for message preparation monitoring and control of the DDS. The DDS will communicate with MCC and ACC using an IP based network.
FR 5.9	DDS software application will provide the normal operator to publish predefined sets of messages (textual / image) along with information from environmental sensors.
FR 5.10	DDS software application will accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client. Software should be GUI based, and capable to handle up to multiple DDS signage. User should be able to select desired location in Map and this should enable user to see the live status of that specific DDS.
FR 5.11	DDS shall also integrate with the smart city platform at ACC for unified control and monitoring.

TR - 5 Technical Requirements

CARBON MONOXIDE (CO) SENSOR	
TR 5.1	Range of CO sensor shall be between 0 to 20 PPM.
TR 5.2	Resolution of CO sensor shall be 0.1 PPM or better.
OZONE (O3) SENSOR	
TR 5.3	O_3 Sensor shall have a range of at least 0-0.4 PPM.
TR 5.4	Resolution of O_3 sensor shall be 0.001 PPM or better.
NITROGEN DIOXIDE (NO2) SENSOR	
TR 5.5	NO_2 Sensor shall have a range of at least 0-0.2 PPM.
TR 5.6	Resolution of NO_2 sensor shall be 0.001 PPM or better.
SULPHUR DIOXIDE (SO2) SENSOR	
TR 5.7	SO_2 Sensor shall have a range of at least 0-0.7 PPM.
TR 5.8	Resolution of SO_2 sensor shall be 0.001 PPM or better.

CARBON DIOXIDE (CO2) SENSOR	
TR 5.9	CO_2 Sensor shall have a range of at least 0-2000 PPM.
TR 5.10	Resolution of CO_2 sensor shall be 1 PPM or better.
PARTICULATE PROFILE SENSOR	
TR 5.11	Particulate profile sensor shall provide simultaneous and continuous measurement of PM10 and PM2.5 in ambient air.
TR 5.12	Range of PM2.5 shall be 0 to 500 micro gms / cu.m or better.
TR 5.13	Range of PM10 shall be 0 to 1000 micro gms / cu.m or better.
TEMPERATURE SENSOR	
TR 5.14	Temperature sensor shall have the capability to display temperature in °Celsius and °Fahrenheit.
TR 5.15	Temperature range shall be -10° to +65°C.
RELATIVE HUMIDITY SENSOR	
TR 5.16	Range of relative humidity sensor shall be 1 to 100% RH.
TR 5.17	Resolution and units of relative humidity sensor shall be 1% or better.
WIND SPEED SENSOR & WIND DIRECTION SENSOR	
TR 5.18	Wind speed sensor shall have the capability of displaying wind speed in mph, km/h, m/s.
TR 5.19	Range of wind speed sensor shall be 0-60 m/s.
TR 5.20	Range of the wind direction sensor shall be 0° to 360°.
RAINFALL SENSOR	
TR 5.21	Rainfall sensor shall the capability of displaying level of rainfall in inches and millimetre.
TR 5.22	Daily Rainfall range shall be 0 to 99.99” (0 to 999.8 mm).
TR 5.23	Monthly/yearly/total rainfall range shall be 0 to 199” (0 to 6553 mm).
BAROMETRIC PRESSURE SENSOR	
TR 5.24	Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa/mb.
TR 5.25	Range of barometric pressure sensor shall be 540 hPa/mb to 1100 hPa/mb.
NOISE SENSOR	
TR 5.26	Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA.
TR 5.27	Noise sensor shall have resolution of 0.1 dBA.
TR 5.28	Noise sensor shall detect the intensity of the ambient sound in a particular area.
TR 5.29	Nosie Sensors shall be installed for the outdoor applications.
ENVIRONMENTAL SENSOR MANAGEMENT SOFTWARE	
TR 5.30	Existing software for environmental sensors is of PAQS make. Environmental sensors installed at Bidkin shall be integrated with the PAQS software.
TR 5.31	Environmental sensors shall be integrated at the ACC with smart city platform via environmental sensor management software for the purposes of monitoring, display of information and control of the system.

DIGITAL DISPLAY SCREEN (DDS)	
TR 5.32	The DDS shall be installed at location identified by Client. The DDS shall be outdoor rated.
TR 5.33	DDS shall have be True Colour. Text on the DDS shall be readable in bright sunlight.
TR 5.34	The pixel pitch of DDS shall be minimum 5mm.
TR 5.35	The lattice density of DDS shall be minimum 27000 dots/square meter.
TR 5.36	The viewing distance shall be between 4m to 30m. The screen size shall be proposed accordingly to ensure that the character height is at least 50mm.
TR 5.37	The average power consumption shall not exceed the 740W/square meter.
TR 5.38	The horizontal view angle shall be > 140 degree.
TR 5.39	The working temperature shall be between 0℃ to +60℃ & humidity shall be between10% to 90%.
TR 5.40	The DDS shall have a Power Supply unit to support AC 110-240 V.
TR 5.41	The MTBF of DDS shall not be less than 100,000 hours.
TR 5.42	The grey scale shall be 16 bit per colour.
TR 5.43	The Brightness shall be 5500 cd/square meter.
TR 5.44	The blind spot rate shall be minimum < 0.00001.
TR 5.45	The IP rating shall be minimum IP65 for front and IP 54 for rear.
TR 5.46	Message shall be readable even in broad daylight without any shade & displayed image shall not appear to flicker to the normal human eye (>5500 cd/m2).
TR 5.47	The Display capability of DDS shall be fully programmable, full colour, full matrix, LED displays & shall have Alpha-numeric, Pictorials, Graphical & video capabilities.
TR 5.48	The Display Language shall be support both pictograms and bilingual (English and Devanagari) text.
TR 5.49	The Display Front Panel shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean & shall be 100% anti-glare via the panel or through an external housing.
TR 5.50	The message Creation shall be through both MCC and ACC Application and locally.
TR 5.51	The DDS shall support Multilingual (Marathi/English/Hindi etc.) languages and all fonts supported by Windows.
TR 5.52	The DDS shall have the facility of auto dimming adjusts to ambient light level.
TR 5.53	The Display size of DDS shall be minimum 70 inches diagonal.
TR 5.54	The DDS shall have the access control mechanism so that the usage is regulated.
TR 5.55	The DDS shall be wall, Pole & gantry mounted. The mounting accessories as well as mounting equipment (pole or gantry) shall be the part of DDS.
TR 5.56	The DDS shall have automatic on/off operation.
GENERAL	
TR 5.57	Each environmental sensor shall be housed in modules and further integrated into one single enclosure.
TR 5.58	The design shall be modular in nature which shall have the capability to add additional environmental sensors in the future into the enclosure.
TR 5.59	It shall be possible to remove or replace individual sensor modules without affecting the functioning of rest of the system.
TR 5.60	It shall be possible to mount the air quality monitoring station to a pole, tripod or wall mounting brackets. Mounting equipment as well as accessories shall be under the scope of MSI.

ENVIRONMENTAL REQUIREMENTS	
TR 5.61	Enclosure shall be rugged weather proof IP65 rated and shall house the power modules, thermal management system, embedded PC and user configured analyser modules as well.
TR 5.62	Environmental operating range shall be 0°C to +60°.
ELECTRICAL REQUIREMENTS	
TR 5.63	Power requirements of the system (environmental station and DDS) shall 220-240 VAC, 50Hz. It shall have an in-built NEMA 5-15P plug factory installed.
TR 5.64	All modules inside the enclosure shall operate from 12VDC power. The MSI shall be responsible for any power conversions required for operations of this system.
NETWORKING REQUIREMENTS	
TR 5.65	Environmental station and DDS shall support communications by Ethernet (RJ45) or Fibre optic communications or 3G/4G.

2.2.6 Solar Panel with Batteries

2.2.6.1 Pole Mounted Solar PV Module

Overview

The solar PV module shall include solar panel, controller, batteries, etc. and shall provide the secondary power to all field devices (i.e. ruggedized switches) mounted on the existing streetlight pole, as required to support the power connectivity needs of this project. Solar PV module shall be installed at all streetlight poles that have co-located field equipment.

BR - 6 Business Requirements

BR 6.1	The solar PV module shall be used to fulfil the independent power requirement of field devices with battery bank and network switch mounted on streetlight pole as required.
BR 6.2	All field equipment mounted on streetlight poles and kiosks, and provided as part of this project shall use solar panel as secondary source of power. The raw power shall act as the primary source of power for all field equipment mounted on streetlight poles and kiosks, and provided as part of this project.
BR 6.3	The capacity of batteries required shall be calculated based on the equipment load and run-time.
BR 6.4	Since the primary source of power to field switch and other equipment will be the raw power supply, all power conversions and ensuring the respective field switches and equipment can be powered by solar (in events of unavailability of raw power) will be factored in while proposing the respective equipment.
BR 6.5	The raw power shall be the primary source of power with solar panel as the secondary source of power. The solar PV module shall ensure that there is seamless transfer between raw power and solar power for every connected equipment without any damage to the equipment or any downtime.

FR - 6 Functional Requirements

FR 6.1	The solar panel shall have crystalline silicon high power solar cells and must have a certificate of testing conforming to IEC 61215 Edition II/ IEC 61730/ TUV Safety Class-II/ BIS 14286 from an NABL (National Accreditation Board for Testing & Calibration Laboratories) or IECQ (International Electro-technical Commission Quality Assessment System for Electronic Components) accredited Laboratory.
FR 6.2	The module efficiency shall not be less than 14%.
FR 6.3	The module should be supplied with screw less hollow section frame and should have limited extended warranty of minimum 25 years.
FR 6.4	The terminal box on the module shall be designed for long life out door operation in harsh environment and shall have a provision for opening for replacing the cable, as required.
FR 6.5	All necessary arrangements to meet the power requirements including electrical wires/ cables required for connections with the nearby distribution board shall be provided with the solar controller.
FR 6.6	The Battery shall be Lithium Ion (Lithium Iron Phosphate $LiFePO_4$) maintenance free C-10, specifically tested for solar applications, with a minimum rating of 12V/ 24V at C-10 discharge rate and shall conform to the latest BIS/ International standards and must have a certification of CE, RoHS & UN 38.3.

	The battery shall be in an isolated and waterproof casing with IP56 protection and have a minimum calendar life of 10 years.
FR 6.7	Any left out specification for the Solar PV widget shall be as per the latest MNRE Guidelines for off-grid and decentralized solar applications.
FR 6.8	Necessary lengths of wires/cables, switches suitable for DC use and fuses should be provided.
FR 6.9	All components (Solar panel, batteries, switching unit and solar controller) must match each other in terms of voltage and intensity of current, and shall be compatible with each other.

TR - 6 Technical Requirements

TR 6.1	The Solar PV module shall be as per the configuration specified below: • Type of cell: Mono/ Multi crystalline silicon; • Front Face: Tempered Glass (Low Iron); • Encapsulate: Ethylene Vinyl Acetate; • Frame: Anodized Aluminium; • Cell Temperature: 25^0C; • Irradiance: 100 mW/cm^2 AM 1.5Power (Pm) (nominal): As per the design requirements.
TR 6.2	Protective devices against surges at the PV module shall be provided. Low voltage drop bypass diodes shall be provided and if required, blocking diode(s) may also be provided.
TR 6.3	The PCB containing the electronics should be capable of solder free installation and replacement.
TR 6.4	Depth of discharge (DOD) of battery shall be minimum 95% i.e., 95 % of the rated capacity of the battery should be between fully charged and load cut off conditions. MSI shall mention the design cycle life of batteries at 100% and 80% depth of discharge (DOD) at ambient temperature up to 40^0C.
TR 6.5	Battery shall have minimum 2000 cycles at 100% DOD & 3000 cycles at 80% DOD.
TR 6.6	The self-discharge of the batteries shall be less than 3% per month at 20^0C and less than 6% per month at 30^0C.
TR 6.7	Battery shall have minimum backup of 4 hours.
TR 6.8	Any cabinet provided as part of the PV module shall be a vented, acid proof and corrosion resistant powder coated metallic cabinet (IP 55 rated) made of CRCA sheet of 2 mm thickness with lockable arrangements. The cabinet shall be supplied with suitable mounting arrangement on pole.
TR 6.9	The system shall have two indicators, green and red. The green indicator shall indicate the charging under progress and should glow only when the charging is taking place. It shall stop glowing when the battery is fully charged. Red indicator shall indicate the battery “Load Cut Off” condition.

2.2.7 IT and Other Common Infrastructure

2.2.7.1 Data Security

The smart city network architecture shall adopt an end-to-end security model that protects data and infrastructure from malicious attacks, thefts, natural disasters, etc. The architecture shall be implemented in such a way that the system is protected from hackers and other threats. The data security system shall address security policies, hardware and software, along with the connectivity between the field device and the respective application. Data Security for AURIC-Bidkin shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).

Note that the client at its discretion may have the authority to carry a security audit of the entire system during the course of the Project or post implementation at regular intervals.

TR - 7 Technical Requirements

ARCHITECTURE	
TR 7.1	The platform shall comprise of high performance purpose built next generation multi-tenant hardware with multicore CPU support. The platform shall support multiple network functions including Application Load Balancing, Application Firewall and Next Generation Firewall functions with dedicated hardware resources for each virtual instance.
TR 7.2	The Platform shall have option to support 3rd party network functions.
TR 7.3	The appliance shall have minimum Four (4) 1G Copper and Four (4) 10G SFP+ data interfaces along with one (1) 1G copper dedicated management interface.
TR 7.4	The appliance shall support minimum 128GB RAM, 2TB HDD and two (2) SSL ASICS/ FGPA/Cards with network virtual function support.
TR 7.5	Next generation multi-tenant platform shall support traffic isolation, fault isolation and network isolation in order to meet the architectural environment. Each network function shall 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.
TR 7.6	Initial phase of the Contract has limited connectivity requirement between Shendra and Bidkin Phase-1. It shall be noted that the MSI shall be responsible to provide the requisite security infrastructure for Bidkin Phase-1 and in case required migrate partial infrastructure to Shendra when the Client has dedicated fibre optic link between Shendra and Bidkin Phase-1.
APPLICATION LOAD BALANCER	
TR 7.7	The Application Load Balancer shall be able to load balance both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.
TR 7.8	The appliance shall 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.
TR 7.9	The appliance shall enable script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP. Load balancer shall also support ePolicies to customize new features in addition to existing features/ functions of load balancer.
TR 7.10	The Application Load Balancer shall provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware shall support both 2048 and 4096 bit keys for encrypted application access.
TR 7.11	The appliance shall support certificate parser and solution shall integrate with client certificates to maintain end to end security and non-repudiation.

TR 7.12	The appliance shall support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".
TR 7.13	The appliance shall provide full IPv6 support.
TR 7.14	The appliance shall support site selection feature to provide global load balancing features for disaster recovery and site redundancy.
TR 7.15	Global load balancing shall support advanced functions Authoritative name sever, DNS proxy/ DNS NAT, full DNS server with DNSEC, DNS DDoS, application load balancing.
TR 7.16	The device shall be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.
TR 7.17	The appliance shall support advance ACL's to protect against network based flooding attacks. Administrator shall able to define ACL's rules based on Connections Per Second (CPS) and Concurrent Connections (CC), cookie value.
TR 7.18	The appliance shall support License upgradable feature to provide machine authentication based on combination of HDD ID, CPU info and OS related parameters, i.e. MAC address to provide secure access to corporate resources.
TR 7.19	The appliance shall support integrated firewall module to protect the device itself from network based DOS and DDoS attacks.
TR 7.20	The appliance shall support the following: • SAML secure application access; • Web Single Sign-On (SSO); • Serves as a SAML SP (service provider).
TR 7.21	The appliance shall have security features like reverse proxy firewall, Syn-flood and DDOS attack protection features.
WEB APPLICATION FIREWALL (WAF)	
TR 7.22	Web Application Firewall should be ICSA certified.
TR 7.23	Web Application Firewall shall be IPv6 ready logo Phase 2 certified.
TR 7.24	The WAF shall use an Intelligent Detection advanced machine learning technology for identifying web attacks, minimizing false positives/ negatives and delivering next-gen real-time web security.
TR 7.25	The Web Application Firewall shall provide bi-directional protection against sophisticated threats like SQL injection and cross-site scripting, and shall also support OWASP application security methodology.
TR 7.26	The solution shall support compliance reporting and support for PCI DSS.
TR 7.27	WAF system shall be able to signal cloud based anti-DDoS system and swing traffic for mitigation of volumetric DDoS attacks.
TR 7.28	The solution shall support integration of Web Vulnerability Systems scanner for fastest time for 0-Day vulnerability mitigation by automatically creating virtual patching policies foremost found vulnerability.
TR 7.29	The MSI shall have their own cloud based Web Vulnerability Scanning System to integrate with WAF for smart patch.
TR 7.30	The solution shall support web page defacement.
TR 7.31	The solution shall support Botnet protection.

TR 7.32	WAF system shall be able to collaborate with anti-DDoS solution to mitigate downtime risk of websites. Once TCP flooding traffic reaches the preset threshold in WAF, the WAF shall be able to automatically notify anti-DDoS from upstream to divert and e risk of websites. Once TCP flooding traffic reaminimize latency issues.
ANTI-DDoS SOLUTION	
TR 7.33	The solution must be a purpose-built appliance based solution with fully hardened and secured Operating System (OS).
TR 7.34	The solution shall be deployed either Out-Of-Path (preferred) or inline (with bypass). Also, the solution must not impede valid network traffic.
TR 7.35	The solution shall support scalable performance through license, and allow the users to upgrade the mitigation capacity without changing the physical hardware.
TR 7.36	The solution shall consist of detector, mitigator and management device.
TR 7.37	The DDoS mitigation devices shall be able to work independently when there is any problem with the DDOS detector.
TR 7.38	The Detector and Management solution shall have dedicated instance on a Network function virtualization platform.
TR 7.39	The DDoS mitigation device shall support up to eight (8) 10 G SFP+, or 32X1G (Copper or Fibre) ports and one (1) 1G management port.
TR 7.40	The anti-DDoS solution shall support Copper and Fibre built-in fail-open/ fail-close bypass function.
TR 7.41	The solution shall have at least 2 Gbps of throughput scalable up to 10 Gbps on same device with an additional license upgrade for future requirement.
TR 7.42	The solution shall support service availability through functions of service monitoring and protection from DDoS traffic.
TR 7.43	The solution shall be stable and not be affect service availability even upon any system fault.
TR 7.44	The solution shall provide in-line mode and Diversion (off-ramping) / Reinjection (on-ramping) mode for detecting and protecting DDos traffic.
TR 7.45	The solution shall detect any DDoS traffic and mitigate any DDoS attack without interrupting legitimate traffic and customer services.
TR 7.46	The solution shall provide Threat Intelligence Protection to filter blacklisted IP, malware hashes, malicious Web URL command and control. Threat Intelligence Protection system shall also comprise of Threat Intel portal and shall support same/ third party anti-DDoS solution.
TR 7.47	The solution shall provide user defined signatures.
TR 7.48	The solution shall be able to monitor up to 4096 protection group and customize policy (ies) for each protection group.
TR 7.49	The solution shall support a DDoS protection function for VoIP (SIP) protocol.
TR 7.50	The solution shall support protection as a group for several IP addresses.
TR 7.51	The proposed DDoS device shall be able to support high-availability with: • Device (Anti-DDoS) failure detection; • Traffic Re-injection Dead Link; • Gateway and Interface detection.
TR 7.52	The solution shall support various methods of injecting traffic back to the original destination. These method(s) shall be capable of injecting traffic in layer-2 and layer-3 environment.

TR 7.53	The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active.
TR 7.54	The mitigation solution shall support out-of-path deployment enabled by dynamic routing protocols such as BGP, OSPF, ISIS.
TR 7.55	The solution shall support policy based routing (PBR) features.
TR 7.56	For Layer 7 DDoS attacks, the mitigation solution shall support keyword checking to check HTTP keywords such as method, cookie, host, referrer, URL, version, user-agent and x-forwarded-for.
TR 7.57	The solution must able to support real-time configuration changes without impact to service.
TR 7.58	The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2.
TR 7.59	The solution shall provide the latest Management Information Base (MIB) file for SNMP operation.
TR 7.60	The solution should support Layer 7 DDoS detection and mitigation. The mitigation devices should support multiple algorithms for HTTP/ HTTPS attack protection.
TR 7.61	The solution shall support the extension based on growth of the network and at least support expansion of mitigation devices up to 25 devices.
TR 7.62	The solution shall support Layer 7 DDoS detection and mitigation using captcha challenge, JavaScript authentication, URL authentication, cookie authentication, E-TAG Authentication from day one.
TR 7.63	The solution shall support the behaviour based and algorithm based DDoS mitigation.
TR 7.64	The solution shall provide the multi-level DDoS mitigation policy and different mitigation action based on DDOS traffic type.
TR 7.65	The solution shall provide the function to monitor the outbound DDoS attack and co-operate with the mitigation platform to block the outbound DDoS attack.
TR 7.66	The solution shall be an IPv6 ready logo Phase 2 certified.
TR 7.67	The solution shall support report format customization. The solution must be able to generate summary attack report of daily/ weekly/ monthly.
TR 7.68	The solution must be able to send schedule summary attack report of daily/ weekly/ monthly.
SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	
TR 7.69	Next generation platform shall encompass log, packet and end point data with added context and threat Intelligence. It shall also provide complete network visibility through deep packet inspection, high speed packet capture and analysis.
TR 7.70	The MSI shall be responsible for developing SIEM for logs and deep packet inspection.
TR 7.71	The solution shall be a physical appliance form factor with following components: • Management & Reporting; • Normalization & Indexing; • Correlation Engine; and, • Data Management.
TR 7.72	There shall be no limitation on number of devices to be supported. Any addition in number of devices shall have no cost impacts.
TR 7.73	The solution shall 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 shall also have role based access control mechanism and shall be capable of handling the entire security incident lifecycle.

TR 7.74	Real time contextual information shall be used at collection/ normalization layer and also shall 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 asset like IP/ Device etc.
TR 7.75	All logs that are collected shall be studied for completeness of information required, reporting, analysis and requisite data enhancement. The solution shall also be able to perform normalization to meet the reporting and analysis needs.
TR 7.76	A single log appliance shall support minimum 30,000 EPS and packet appliance shall support up to 1 Gbps line rate with multiple ingress interfaces for capturing from multiple network interfaces.
TR 7.77	Correlation Engine appliance shall be consolidated in a purpose build appliance and shall be able to handle 100,000 EPS.
TR 7.78	The solution shall be able to store both raw logs as well as normalized logs. The same shall be made available for analysis and reporting. The solution shall be scalable to provide online storage for 1 year at central site.
TR 7.79	The solution shall incorporate and correlate information that enables the Information Security Team to quickly prioritize its response to help ensure effective incident handling.
TR 7.80	The monitoring shall be cross-device and cross-vendor and shall be both out of the box and scalable to cover additional devices and applications as required.
TR 7.81	Appliance shall have minimum 128 GB RAM to provide optimal performance and shall also provide at least four (4) network interfaces onboard.
TR 7.82	The appliance shall be managed and monitored from SIEM unified console for Correlation, Alerting and Administration.
TR 7.83	The appliance shall be able to store raw packet data for seven (7) days and normalized packet data for 30 days for forensics.
TR 7.84	The appliance shall be able to provide complete packet-by-packet details pertaining to one or more session of interest including: Session replay, Page reconstruction, Image views, Artefact & raw packet and Object extractions.
TR 7.85	The solution shall be able to filter the captured packets based on layer-2 to layer-7 header information.
TR 7.86	The solution shall provide comprehensive Deep Packet Inspection (DPI) to classify protocols and application(s).
TR 7.87	The proposed solution must be able to provide the complete platform to perform Network forensics solution.
TR 7.88	The solution must be able to: • Detect malicious payload in network traffic; • Detect and reconstruct files back to its original type; • Detect hidden or embedded files; • Detect and flag out renamed files. The solution must also have the ability to capture network traffic and import PCAP files using the same infrastructure.
ANTIVIRUS AND FIREWALL	
TR 7.89	The Antivirus solution shall provide enhanced antivirus protection for desktops, laptops & servers of all the attacks originating from places inside/ outside of the network due to virus and/or other malicious programming code and should give appropriate warning messages.
TR 7.90	Solution shall able to detect and block malicious software (in real time) including viruses, worms, trojan horses, spyware, adware, and RootKit.

TR 7.91	The Antivirus solution shall be able to automatically scan external devices (Floppy disks, Compact disks, USB devices and network shares in real-time when accessed) as soon as they are attached to PC, Server, Laptop etc.
TR 7.92	Anti-Virus software must have the capability to clean, Quarantine or delete viruses and shall be able to detect new classes of viruses by normal virus definition update mechanisms.
TR 7.93	The Antivirus solution technology shall include a behavioral based technology apart from providing the signatures for vulnerability add heuristic based approach. It shall be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule -based configurations to provide protection from unseen threats, i.e. zero-day threats.
TR 7.94	The Antivirus solution shall be able to scan compressed file formats like zip, arj gzip, bz2, jar, rar, lhz, tar Microsoft Compressed Tile etc.
TR 7.95	The Antivirus solution shall have a Centralized Management Console and shall be able to manage the anti-virus programs on the network from a single web-based console.
TR 7.96	Antivirus solution shall be capable of deploying Antivirus on all desktops and servers attached to the network centrally. It shall also be able to generate the information reports such as Antivirus coverage, Virus definition update, Virus infection detected and action performed etc.
TR 7.97	The Antivirus solution must provide a mechanism for developing and deploying policy to each system node with respect to scheduling scan jobs, real-time scan settings, signature distribution, alerting and analysis etc.
TR 7.98	The Antivirus solution shall support multi -platform Operating System (Windows, Mac, Linux) and the same shall be managed from a single Centralized Management Console.
TR 7.99	Antivirus solution shall support integration with Active directory for directory structure of computers for better management, and shall have logical group based on IP addresses (Subnets).
TR 7.100	Antivirus solution shall have a single, configurable installation with centralized configuration and policy management. It shall also have a Common Distribution Mechanism via combination of push & pull technology for better BW management.
TR 7.101	Antivirus shall be capable of pushing client installation from a centralized location and it shall also support manual installation of client via network share.
TR 7.102	Antivirus shall provide centralized event logging to locate and cure virus problems.
TR 7.103	Administrator shall be able to initiate virus sweeps remotely in case of an outbreak.
TR 7.104	Administrator shall have flexibility to schedule scan and update at the endpoints from central server.
TR 7.105	Administrator must be able to distribute new and updated anti-virus software, virus definitions and Policies automatically to clients and servers from a central location.
TR 7.106	Antivirus shall provide a feature for the roll-back of malware actions during disinfection (Roll back means rolling back the changes made to the file system (creating, relocating, renaming files) and registry keys.
TR 7.107	Solution shall provide web antivirus features which shall analyze site address and block access to dangerous sites and scan the object downloaded over HTTP.
TR 7.108	Solution shall provide mail antivirus features which shall protect from the threats that e-mail message may contain and messages shall be successfully intercepted at the protocol level (POP3 & SMTP level) and by embedding into the most popular mail clients.
TR 7.109	Solution shall provide a web console feature that works via a browser (the web console shall be used for creating reports and performing simple operations with computers i.e. viewing the status, relocating, installing Antivirus.
TR 7.110	Solution shall provide application privilege control to regulate the activities of the running programs, namely, access to the file system and registry as well as interaction with other programs.

TR 7.111	Antivirus solution shall provide Application startup Control module with the ability to grant, block and audit application launch based on administrator-applied policies.
TR 7.112	Antivirus solution shall provide device control module with ability to control usage of unknown or unwanted devices, reducing the risk of data loss, White list categories (based on serial numbers) & temporary grant access to access block device.
TR 7.113	Solution shall provide tamper protection features i.e. user who does not know the password may not able to change the existing policy, exit or uninstall the antivirus solution.
TR 7.114	The proposed solution shall have predefined rules for hundreds of the most commonly used applications reduce time spent on configuring the firewall.
TR 7.115	The Firewall module should have rule-based approach with administrator defined rules.
TR 7.116	The Firewall module should have feature(s) to allow or block certain network traffic, based on port-number/ protocol and based on network address.
TR 7.117	The Firewall module shall monitor the traffic from the applications installed on that endpoint. Specific rules can be created to block certain application's network traffic.
TR 7.118	The solution shall support Host Intrusion Prevention System (HIPS) module which could protect the endpoint from network based attacks. The signatures for HIPS shall be regularly updated to identify latest network attacks for endpoints.
TR 7.119	The endpoint solution shall have a feature to detect network attacks originating from a computer, and then further be able to block the traffic from that computer.
TR 7.120	The Firewall module shall have option to create network subnets like Public, Trusted, Local etc. and accordingly the network traffic flowing rules shall be created.
TR 7.121	The Firewall module shall have option to automatically categorize the applications in Trusted, Low Restricted, High Restricted, Untrusted etc. and accordingly the application's network traffic should be allowed.
TR 7.122	Firewall shall allow creation of inbound or outbound traffic restriction rules.
TR 7.123	Alerts on virus activity shall be passed on to Administrator.
TR 7.124	Antivirus solution shall provide web control module with the ability to monitor and filter users' browser activities by category, content and data type regardless of workstation location.
TR 7.125	Solution shall provide mobile device security and Mobile Device Management (MDM) feature. It shall also support Active Directory, Microsoft Exchange ActiveSync and Apple MDM Server.
TR 7.126	Solution shall provide management visibility and security for mobile endpoints without the complexity of a separate solution.
TR 7.127	Solution shall provide antimalware feature for mobile devices and shall use the power of the cloud to provide rapid protection against new and emerging threats.
TR 7.128	Solution shall provide multi-level defense technologies for mobile devices (E.g. Anti-spam technology to filter out unwanted calls and text messages). It shall also have safe browser feature for iOS devices to protect against phishing websites.
TR 7.129	Solution shall have feature to enforce encryption on each user's mobile device and shall offer a convenient way to enforce the use of the encryption technologies that are resident within the mobile device in order to ensure that all data on the device is encrypted that's held within a special container on the user's device.
TR 7.130	Solution shall support Bring Your Own Device (BYOD) initiatives and shall include containerization features to help ensure corporate data and personal data held in separate containers on the user's device.
TR 7.131	Solution shall have special anti-theft features that shall help minimize the risk of security breaches that can result from a lost or stolen device.

TR 7.132	Solution shall have remote lock, locate and wipe features (E.g. Administrator can remotely lock a mobile device, find the device's approximate location). the Administrator shall also able to choose to wipe corporate data from the device and return the device to its original factory settings.
TR 7.133	Solution shall have Self-Service Portal for anti-theft, so users can rapidly respond to loss of a device and reduce the risk of data loss and avoid load on administrators.
TR 7.134	Solution shall have a feature which can help Administrator in controlling a lost device even when its SIM has been changed.
TR 7.135	Solution shall have a Mobile Device Management (MDM) feature with extensive mobile device management functionality to give Administrator easy and rapid control over all mobile security functions.
TR 7.136	Solution shall have boosting systems management capabilities plus an array of security technologies that can be managed and controlled from one management console.
TR 7.137	Solution shall have a feature for the creation and cloning of computer images to save time and help to optimize operating system deployment. Images shall be stored in a special inventory and it shall be ready for access during deployment.
TR 7.138	Solution shall have an Application provisioning feature E.g. Administrator can deploy third party software on command or can schedule it for outside normal office hours. The software deployment process shall be entirely transparent to users.
TR 7.139	Solution shall have a License Provisioning and Control feature (E.g. centralized license provisioning and tracking of any breaches of license conditions).
TR 7.140	Solution shall have Asset management feature for hardware and software (E.g. all devices and software on the network shall be automatically discovered and recorded in hardware and software inventories).
TR 7.141	Solution shall have Patch Management features – Advanced in-depth scanning for vulnerabilities combined with the automated distribution of patches.
TR 7.142	Solution shall have a remote troubleshooting and deployment tool i.e. it shall help Administrator to resolve problems efficiently. Furthermore, the Administrator shall be able to deploy a new software remotely by reducing the load on his network by using one local workstation as the update agent for the whole site.
TR 7.143	Solution shall have full-disk, file level and removable media backed by Advanced Encryption Standard (AES) with 256 bit encryption to secure critical business information in the event of device theft or loss.
TR 7.144	Full Disk encryption shall operate on the physical sectors of the disk to deliver encryption that's 'close to the hardware' and also enable an 'encrypt everything at once' strategy.
TR 7.145	File level encryption shall offer granular encryption of individual files and help to enable secured sharing of data across the network.
TR 7.146	Solution shall have a feature to increase security through policies that enforce the encryption of data on removable devices.
TR 7.147	Solution shall support Portable Mode for File Level Encryption on removable media.
TR 7.148	Users shall be able to create password-protected, encrypted, self-extracting packages of files and folders. This shall enable the secure transfer and sharing of sensitive data – via a removable device, email or the web.
TR 7.149	Administrator shall be able to access vital encrypted data in the event of a system failure – even if the operating system is unable to boot.
TR 7.150	If a user loses or forgets their password, a challenge / response mechanism shall allow the recovery of the pre-boot password to access the encrypted data.

HOST INTRUSION PREVENTION SYSTEM (HIPS)	
General	
TR 7.151	Physical, Virtualization & Cloud systems shall be managed from a single console.
TR 7.152	Anti-malware software for virtual environments shall include the below: • Agentless anti-malware software for VMWare environments; • Light Agent based anti-malware software for virtual environments; • Agent based solution for Public Cloud; • Centralized management, monitoring and updating of software; • Ability to update anti-malware databases and network attack patterns; • Administrator and User documentation in English; • Software defined networking compatibility.
Management Console	
TR 7.153	The solution shall enable installation of anti-malware software from a single distribution.
TR 7.154	The solution shall support selection of installation depending on the number of protected nodes.
TR 7.155	The HIPS module shall enable the following: • Centralized installation; • Updation and removal of anti-malware software; • Configuration, administration, viewing of reports; and, • Statistical information about operation.
TR 7.156	The software shall enable centralized removal (manual and automatic) of incompatible applications from the administration center.
TR 7.157	The RPC and GPO methods of anti-malware agent installation shall be supported by the HIPS module along with an administration agent for remote installation. The solution shall also have the option to create a standalone installation package for local installation.
TR 7.158	The HIPS module shall enable remote installation of anti-malware software with the latest anti-malware databases.
TR 7.159	The following functionalities of automatic update of anti-malware software and anti-malware databases shall be provided as part of the HIPS module: • Automatic search for vulnerabilities in applications and the operating system on protected machines; • Ability to manage the component prohibiting the installation and/or running of programs; • Ability to manage the component controlling work with external I/O devices; • Ability to manage the component controlling user activity on the Internet; • Testing of downloaded updates by means of the centralized administration software prior to distributing them to client machines; • Delivery of updates to user workplaces immediately after receiving them; • Ability to execute an automatic deployment based on the request of the dedicated protection system for virtual infrastructures; • Creation of a multi-level administration system that allows administrator and operator roles to be set, as well as the reporting forms for each level.
TR 7.160	The HIPS solution shall support the following system functionalities: • Automatic Exploit Prevention; • Light Agent Support (for low impact on the performance);

	• File antivirus protection; • Network attack blocker; • URL Scanning; • Scanning of protocols POP3/SMTP/NNTP/IMAP; • Prevent startup of applications using specialy configured rules; • Default deny support; • Checking of files during anti-malware scan irrespective of file size; • Exporting the files into CSV, HTML , XML , PDF and RTF formats; • Agent Built-in Web Control, Mail Antivirus, IM (Instant Messaging) antivirus, Device Control, Automatic Exploit Prevention, Application privilege control, Watchdog technology; • Direct anti-malware database updates from management server for SVA; • Should have dedicated Security Virtual Appliance; • Support for VDI infrastructure; • Support Built-in Redundancy techniques to allow reconnecting to any SVA within the infrastructure without any manual (re)configuration; • Support changes in SVA configuration without SVA re-installation; • Support file execution/launch notification; • Protection against malware in real-time and during scheduled scanning without installing an anti-virus agent on guest virtual machines.
TR 7.161	The Agent based anti-malware software for virtual environments shall meet the following functionalities: • Resident anti-malware monitoring; • Protection against rootkits and auto dialers to paid sites; • Heuristic analyzer to detect and block previously unknown malware; • Transfer of anti-malware scanning and other resource-intensive tasks from all guest virtual machines to a separate machine; • Ensuring continuity of file protection during short-term unavailability of the protection machine by logging all file operations on the protected virtual machine during the period of unavailability, and automatic scanning of all changes after access is restored; • Cloud-based protection against new threats, allowing the application to access a developer's special resources in order to obtain file verdicts during real-time or scheduled scanning; • Protection of e-correspondence from malware by checking incoming and outgoing traffic on IMAP, SMTP, POP3, MAPI, NNTP protocols regardless of the email client; • Protection of web traffic (scanning of objects including the use of heuristic analysis sent to the user's computer via HTTP and FTP protocols) with the ability to configure trusted sites; • Blocking banners and pop-ups on web pages; • Detection and blocking of phishing sites; • Protection against yet unknown malicious programs based on their behavior; • Ability to determine anomalous behavior by an application by analyzing its execution sequence; • Ability to roll back malware operations during treatment; • Built-in firewall that allows network packet rules to be set for specific protocols (TCP, UDP) and ports; • Creation of network rules for specific programs; • Protection against hacker attacks by using a firewall with an intrusion detection and intrusion prevention system (IDS/IPS) and network activity rules for the most popular applications when working on any type of computer networks, including wireless networks;

	• Component enabling the creation of special rules to block the installation and/or running of a program. The component should be able to control the application via program path, metadata, MD5 checksum, and predefined categories of applications provided by the vendor. It should also allow exceptions to the rules for specific AD users; • Monitoring user activity with external I/O devices by the type of device and/or the bus used including the ability to create a list of trusted devices by their ID and the ability to grant privileges to use external devices to specific AD users; • Monitoring user activity on the Internet including blocking or permitting access to certain resources as well as the ability to block certain types of information (audio, video, etc.). The software shall allow the implementation of time intervals for control, and the ability to assign them only to specific AD users; • On-schedule scanning of all virtual machines; • Availability of information about scanned files on the protection machine to prevent re-scanning of the same files on different virtual machines; • Ability to apply different security settings for different groups of virtual machines;
TR 7.162	Agentless anti-malware software for virtual environments shall meet the following functionalities: • Protection against malware in real-time and during scheduled scanning without installing an anti-virus agent on guest virtual machines; • Cloud-based protection against new threats, allowing the application to contact the security vendor's specialized resources for a file verdict during real-time or scheduled scanning; • Centralized updates on the specialized protection machine without the need to distribute updates to each guest machine; • On-demand (or manual) scanning of selected virtual machines (VM); • Scanning selected files, folders or the whole system; • On-schedule scanning of all virtual machines; • Ability to deploy a solution without hypervisor reboot or maintenance mode; • Prevent re-scanning of files; • Prevent re-scanning of the same object on different guest machines within a single host; • Blocking, neutralization and removal of malware, notification of administrators; • Single management console for all protection components; • Support management of endpoints & virtualization via Single Console with no need of additional integration and management solutions; • Detailed information about events on virtual machines and the implementation of tasks; • Ability to apply different security settings for different groups of virtual machines; • Ability to exclude from protection files with a specific name, files located at a specific address and files with a specific mask; • Ability to export/import a list of exceptions; • Ability to exclude network drives from protection; • On-demand scanning of powered-on and powered-off virtual machines;
INTRUSION PREVENTION SYSTEM (IPS)	
TR 7.163	The Firewall shall be appliance based and shall facilitate multi-application environment which shall support current network traffic as well as future growth.
TR 7.164	The Firewall shall belong to a family of products that attains IPv6 Ready Phase 2 & IPv6 Certification.
TR 7.165	The platform shall be based on security-hardened, purpose built operating system architecture that is optimized for packet and application level content processing.
TR 7.166	The IPS shall provide a HTTP, HTTPS, SSH, TELNET, SNMP based management console for managing and configuring various components of the appliance.

TR 7.167	The proposed system shall be able to facilitate administration audit by logging detailed activities to event log for management, configuration changes, updates which shall also enable Admin to boot firmware on the earlier revision / configuration in case of any errors.
TR 7.168	The administrator authentication shall be facilitated by local database, PKI & remote server such as Radius, LDAP, AD and TACS+.
TR 7.169	The Firewall system shall have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution.
Networking and System Performance Requirements	
TR 7.170	The Firewall shall support a minimum of 4 X 1G RJ45, 4 X 1G SFP, 4 X 10G SFP+ & 1 X 1G Management & 1 Console interfaces with auto sensing capacity.
TR 7.171	The platform shall support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
TR 7.172	The solution shall support automatic ISP failover as well as ISP load sharing.
TR 7.173	The Firewall shall support Static, Policy Base, Identity based, Multicast routing and Dynamic routing for OSPF, OSPFv3, BGP4, ISIS.
TR 7.174	The Firewall shall support Static, Policy Based, and Multicast routing.
TR 7.175	The Firewall shall support throughputs of 40 Gbps or better.
TR 7.176	The firewall shall support throughput of at least 25Gbps of AES - IPSEC VPN and should be H/W accelerated.
TR 7.177	The solution shall support concurrent session of at least 5 Mil.
TR 7.178	The solution shall support and IPS throughput of 10GBPS with recommendation profile and at least 10Gbps with production environmental profiles or better with enterprise mix traffic.
Firewall Requirements	
TR 7.179	The Firewall shall support deployment modes as: "Route Mode" or "Transparent Mode" and support web proxy/SSL proxy.
TR 7.180	The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs.
TR 7.181	The Firewall shall support Inbound Port Forwarding with inbound Load Balancing if servers are running in high availability (layer 4).
TR 7.182	The Firewall shall support IPv6 ACL to implement security Policy for IPv6 traffic.
TR 7.183	All internet based applications shall be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc.
TR 7.184	The Firewall shall be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port (i.e. when HTTP is not using standard port TCP/80).
TR 7.185	The Firewall shall support deployment of virtualization at least for 5 virtual context from the day one without any additional cost / licenses & must be upgradable up to 100 by addition license.
TR 7.186	The virtual context must have all security features for use for every single firewall.
Traffic Shaping Requirements	
TR 7.187	The proposed system shall have integrated Traffic Shaping functionality including these features: • Enable and disable traffic shaping per firewall policy; • Setting guarantee bandwidth and maximum bandwidth per firewall policy; • Tag and Pass Differentiated Service tagging;

High Availability (HA) Requirements	
TR 7.188	The HA solution shall support stateful session maintenance in the event of a fail-over to a standby unit(s).
TR 7.189	The HA solution shall support both Active-Active and Active-Passive load balancing.
TR 7.190	The High Availability should be supported in the Firewall from the day one and without any extra license.
Network Intrusion Detection & Prevention (NIDP) System	
TR 7.191	The Network Intrusion Detection & Prevention (NIDP) System shall meet the following functionalities: • Built-in Signature and Anomaly based IPS engine on the same unit and Anomaly based detection should be based on thresholds; • Prevent denial of service and Distributed Denial of Service attacks on signature; • Administrator shall be able to configure DOS policies that are used to associate DOS settings with traffic that reaches an interface based on defined services, source and destinations IP/range; • Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types; • Support at least 5000+ attack signature and should be automatic updates directly over the internet for the newly discovered attacks; • Security check updates do not require reboot of the unit; • Attack recognition inside IPv6 encapsulated packets; • User-defined signatures with regular expressions;
TR 7.192	The Intrusion Prevention System (IPS) shall comprise of the following in context to data collection and management: • Dual Power Supply; • IPS system shall be transparent to network, not default gateway to Network; • Separate interface for secure management; • Protect multi-segment in the network, and shall be able to protect up to 4 segments; • Web Protection; • Mail Server Protection; • Cross-site Scripting; • SNMP vulnerability; • SQL injection; • TCP Reassembly; • IP defragmentation; • Bi-directional inspection; • Forensic data collection; • Access Lists; • Provision for real time updates of Signatures along with support for automatic signature synchronization from database server; • Web device shall have capability to define user defined signatures; • Drop Attack Packets; • Reset Connections; • Packet Logging; • Action per Attack;

	• Alerting SNMP; • Log File; • Syslog; • E-mail; • SNMP v1, v2, v3; • HTTP, HTTPS; • SSH, Console; • Support 24/7 Security Update Service; • Support Real Time signature update; • Support Provision to add static own attack signatures;
Logging and Reporting	
TR 7.193	The solution must have at least 2TB of storage for logging & reporting.
TR 7.194	The solution must be an external device not included in FW, and shall be a passive device which shall not have impact on production.
TR 7.195	The MSI shall integrate the proposed solution with Firewall for seamless operations of the system.
TR 7.196	Proposed solution must have features like Event management, Alert mails, Schedule reporting, FTP/TFTP log transfer etc.

2.2.7.2 Operator Workstations

The operator workstations shall be specifically installed for the operators at the Mini Control Centre. Other than this, there will also be a need to provide Laptops. The specifications for Operator Workstations and different type of Laptop requirements are mentioned below.

Technical Requirements

OPERATOR WORKSTATIONS	
TR 7.197	The workstations shall have a wireless optical mouse with USB connection complying with FCC and CE norms.
TR 7.198	The workstation shall be Energy star 5.0/BEE star certified.
TR 7.199	The workstations shall have a 104 Key English wireless keyboard with USB connection.
TR 7.200	Keyboards, Mouse and accessories shall be connected via respective signal extender as required.
TR 7.201	Workstation shall have a standard audio sound card and speakers.
TR 7.202	The workstations shall have an Intel Core i7–8700, six core processor with 3.20 GHz or better or equivalent 64 bit x 86 processor.
TR 7.203	The workstations shall have at least 8 GB DDR3 memory @ 2666 MHz.
TR 7.204	The workstations shall have a min. of 4 DIMM slots supporting up to 64GB ECC. One DIMM Slot must be free for future upgrade.
TR 7.205	The workstations shall have a min. 1 TB SATA III hard disk @ 7200 RPM or higher.
TR 7.206	The workstations shall have shall two colour LED monitors of minimum 24” diagonal non-glare screen and a dual AMD Radeon Pro WX2100 (2GB memory size, 48 Gbps memory bandwidth) professional graphics card with mDP and DP ports or better.
TR 7.207	The workstations shall have graphic accelerator of ATI Rage Pro/AGP graphics accelerator, 4 MB SDRAM.
TR 7.208	The graphics card shall have a minimum resolution of 2560 x 1440 with 5ms response time or better specifications.
TR 7.209	The workstations shall have a DVD multi burner and Dual Layer DVD-RW as an internal optical drive or better.
TR 7.210	The workstations shall have an industry-standard professional-grade operating system. Acceptable systems include Microsoft Windows 10 or better.
TR 7.211	The workstations shall have at the minimum ports: 1 serial, 6 USB 2.0 or higher with 2 in the front, integrated autosensing RJ-45 network interface, and Line-In/Mic In and Line-out/speaker Out (3.5 mm) audio in/out jacks.
TR 7.212	The workstations shall have an expansion bus of 3 PCI/ PCIe Slots; 4 ISA Slots (3 slot shared).
TR 7.213	The workstations shall have Microsoft Office Professional and Antivirus.
TR 7.214	Other pre-loaded software (open source/ free) shall be Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered).
TR 7.215	The AC input power shall be 220-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 7.216	The workstations shall have a dual port 1 Gbps Ethernet network interface card.
TR 7.217	The workstation shall be operational in temperature between ten degrees Celsius (10°C) to thirty degrees Celsius (30°C).

TR 7.218	The workstation shall be loaded with advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server.
LAPTOPS	
Laptop: Type I	
TR 7.219	The MSI shall provide Microsoft Surface Pro 6 laptop devices with the following configuration: • Intel i7-8650U processor with Intel UHD Graphics 620 card; • 512GB SSD storage with 16 GB RAM; • 12.3 inches Display; • Operating System (OS): Windows 10 or better; • 5.0MP front-facing camera with 1080p HD video; • 8.0MP rear-facing autofocus camera with 1080p full HD video; • One (1) full-size USB 3.0 port; • 3.5 mm headphone jack; • Mini Display port; • One (1) Surface Connect port; • Surface Type Cover port; • MicroSDXC card reader.
TR 7.220	The Microsoft Surface Pro 6 Laptop devices shall be provided with the following standard accessories as a minimum: • Touch screen Pencil / Pen; • Microsoft Wireless mouse; • Protective case.
TR 7.221	The Laptop shall have Microsoft Office Professional and Antivirus.
TR 7.222	Other pre-loaded software (open source/ free) shall be Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered).
Laptop: Type II	
TR 7.223	Laptop shall have an Intel Core i7–8th Gen, four core 64-bit processor with Intel 620 Graphics card.
TR 7.224	The Laptop shall have at least 16 GB DDR4 memory @ 2400 MHz.
TR 7.225	The Laptop shall have a minimum 500GB SSD hard disk.
TR 7.226	The Laptop shall have a minimum of 2 DIMM slots supporting up to 32GB ECC.
TR 7.227	The Laptop shall have a dual port 1 Gbps Ethernet network interface card.
TR 7.228	The Laptop device shall have a display screen of 15.3 inches (FHD) with pixel resolution of 1920X1080.
TR 7.229	The Laptop shall have the following minimum ports: • 1 HDMI; • Three (3) USB 3.0; • Integrated autosensing RJ-45 network interface; • Line-In/Mic In and Line-out/speaker Out audio in/out jacks.
TR 7.230	Laptop shall have a standard audio sound card and speakers.
TR 7.231	The Laptop device shall have Windows 10 Pro as the Operating System (OS).
TR 7.232	The Laptop device shall have Microsoft Office Professional and appropriate Antivirus.

TR 7.233	Other pre-loaded software (open source/ free) shall be Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered).
TR 7.234	The Laptop device shall have the latest version of AutoCAD along with its license.
TR 7.235	The AC input power for the Laptop device shall be 220-240 VAC.
Laptop: Type III	
TR 7.236	Laptop shall have an Intel Core i5–8th Gen, four core 64-bit processor with AMD Graphics R5 M530 graphics card.
TR 7.237	The Laptop shall have at least 8 GB DDR4 memory @ 2213 MHz.
TR 7.238	The Laptop shall have a minimum 500 GB SATA hard disk @ 7200 RPM or higher.
TR 7.239	The Laptop shall have a minimum of 2 DIMM slots supporting up to 16GB.
TR 7.240	The Laptop shall have a dual port 1 Gbps Ethernet network interface card.
TR 7.241	The Laptop device shall have a display screen of 14 inches (HD).
TR 7.242	The Laptop shall have the following minimum ports: • 1 HDMI; • One (1) USB 3.0; • One (1) USB 2.0; • One (1) US 2.0; • VGA Integrated autosensing RJ-45 network interface; • Line-In/Mic-In and Line-out/Speaker-out audio in/out jacks.
TR 7.243	Laptop shall have a standard audio sound card and speakers.
TR 7.244	The Laptop device shall have Windows 10 Pro as the Operating System (OS).
TR 7.245	The Laptop device shall have Microsoft Office Professional and appropriate Antivirus.
TR 7.246	The AC input power for the Laptop device shall be 220-240 VAC.
iPad Mini 4	
TR 7.247	iPad Mini 4th Generation shall have memory of at least 64 GB.
TR 7.248	iPad Mini shall support both Wi-Fi and cellular communications.
TR 7.249	iPad Mini shall come with a protection case.
TR 7.250	iPad Mini shall come with all standard accessories.

2.2.7.3 Communication Cabinets with Racks

The cabinets shall be installed at MCC and PoP rooms. The cabinets shall be capable of accommodating all the network devices to support the design requirements.

Technical Requirements

COMMUNICATION CABINET WITH RACKS	
TR 7.251	The cabinets shall be capable of accommodating all the network devices to support the design requirements and shall include at least size 42U racks.
TR 7.252	All cabinets shall be supplied with standard 19” wide rack mount assemblies that shall allow for

	mounting of standard rack-mount equipment.
TR 7.253	All cabinets shall be supplied with standard lockable doors.
TR 7.254	The cabinets shall be IP55 rated.
TR 7.255	All cabinets shall have provision for cable entry from top & bottom of rack with knock-off, pre-punched marked openings.
TR 7.256	All cabinets shall have vertical cable managers in front with suitable accessories on each side of the rack with covers for concealed wiring within the rack.
TR 7.257	Front door shall be made of Tinted toughened glass and should be lockable.
TR 7.258	All cabinets shall have equipment mounting frame (rail notches) for mounting of equipment.
TR 7.259	Shelves for equipment placement shall be provided as required.
TR 7.260	All cabinets shall be designed to carry the anticipated load of all equipment that shall be installed inside the cabinet with at least 30% spare per rack.
TR 7.261	All cabinets shall be provided with standard accessories including vertical and horizontal cable manager, lights, fans, and power bars as needed to support the design requirements of this Project.
TR 7.262	The rack shall have ventilation louvers or uniform perforations on side panel & rear door & equipment cooling with fans (4nos.) housed in fan trays.
TR 7.263	Two strips each with minimum 8 numbers of 5A/15A, 230 VAC power outlets with MCB, inbuilt surge suppressor & line filter for conditioned power output shall be provided.
TR 7.264	The device shall support operating temperature range of 5°C to +40°C.
Outdoor Enclosures (As needed)	
TR 7.265	Minimum 6RU weather proof NEMA 4X/IP65 compliant UV resistant outdoor metallic enclosure in conformance with DIN 41494.
TR 7.266	Vandal proof design with single side door and with minimum IP 55 compliant industrial lock.

2.2.7.4 Servers

Technical Requirements

SERVERS	
TR 7.267	Servers will be provided to support local processing and storage as per the requirements of this RFQ cum RFP.
TR 7.268	A sufficient number of physical servers shall be provided such that their CPU, RAM, and other key server component performance do not exceed 50% utilization individually.
TR 7.269	The MSI shall provide sufficient amount of storage to support the operational needs. The storage on-site shall be for at least 30 business days post which the storage can be archived to on-site media provided by the MSI.
TR 7.270	The server shall have Dual Processor Intel Xeon Scalable Skylake CPU / 8 Core 2.1 GHz or better.
TR 7.271	The server shall have 512 GB of RAM, Configures with 3 TB of storage. The memory shall be scalable to double the capacity configured.
TR 7.272	The Server shall include 2-Hot plug redundant power supplies and cooling fans.
TR 7.273	The Server shall have an Optical Drive 48x SATA CDRW/DVD Combo Drive.

TR 7.274	The Server chassis shall be rack mountable and include rack mounting hardware.
TR 7.275	The Server shall include 12 Gbps Hardware 2Gbps Cache RAID controller (RAID 0, 1, 5, 10) supporting up to eight (8) hot-plug Serial-attached SCSI (SAS) drives.
TR 7.276	The Server shall include hard drives based on volume of data to be stored. The transaction data storage requirements shall be estimated based on total transactions & related calculations as per the functional requirements.
TR 7.277	The Server shall provide either of the following Operating System: • Microsoft Windows Server 2012 / 2016; • Canonical Ubuntu Latest Version; • Cent OS 7.5; • Red Hat Enterprise Linux (RHEL); • SUSE Linux Enterprise Server (SLES); • VMware; • Citrix XenServer.
TR 7.278	Suitable commercial off-the-shelf antivirus software shall be provided for the duration of the contract.
TR 7.279	The central system server shall have a hot standby to mitigate any risk of failure in central system which halts the system performance.
TR 7.280	Server shall be designed to provide a fully redundant and fault tolerant system and shall be available for 99.99% or greater. The unscheduled down time shall be less than 0.01%.
TR 7.281	Server shall be provided with the link load balancers and server load balancers as needed to optimize the overall IT infrastructure operations. The most efficient operations of servers shall be the responsibility of the MSI.
TR 7.282	The Server Management Software shall provide role-based security along with pre-failure warning for: • CPU; • Memory; • HDD.
TR 7.283	The Server shall be provided with redundant hot swappable power supplies. The power supplies shall be FCC Class-A certified.
TR 7.284	The Server shall comprise of redundant fully populated Hot swap fans.
TR 7.285	The Server shall meet the following remote management capabilities: • Manage the server hardware and software components remotely; • Power on/off and boot the system remotely.
TR 7.286	The Server shall comprise of the following interfaces and ports: • 4 X 1 GE (LAN) ports; • 1 X 10 G SFP+ dual port; • 1 X 16GB FC HBA DP; • 1 Serial interface; • 1 VGA interface; 3 USB ports. • 3 PCIe Gen 3

2.2.7.5 Uninterruptable Power Supply (UPS)

The UPS unit shall be provided at each PoP rooms and MCC room (Command and Control Centre and Rack Room) to backup entire AITL devices & switches, emergency lights and Fire detections system. UPS system shall provide a redundant power supply to the following needs:

- Servers and important network and storage equipment;
- Access control, Fire Detection & suppression system and surveillance system.

BR - 7 Business Requirements

BR 7.1	The UPS unit shall be provided with external batteries as needed to support the run-time requirements.
BR 7.2	All AITL equipment installed at PoP and MCC shall be connected on the UPS.
BR 7.3	The quantity of batteries required for the UPS, shall be calculated based on the equipment load and run-time.
BR 7.4	The UPS units shall provide backup power to critical load. In addition, UPS shall also provide cleansed power to these equipment.

FR - 7 Functional Requirements

FR 7.1	The UPS unit shall be 3:1 phase on-line ups with extendable rack system.
FR 7.2	The UPS design shall ensure that a single component/ device failure shall not result in failure of the entire UPS system. The design of UPS System shall be modular to permit easy maintenance.
FR 7.3	The various overload capacities of inverters, static switch, and step down transformer/voltage stabilizer as specified herein are the minimum requirements.
FR 7.4	The UPS system to be supplied by the MSI shall have maximum humming noise level of 65 DB one meter away from the UPS cabinets. This shall not exceed 69 dBA measured 5 feet from surface of the UPS.

Technical Requirements

TR 7.287	The MSI shall provide the calculations to support the UPS rating and number of batteries as part of the bid submission. UPS shall be provided as N+1 physically redundant configuration.
TR 7.288	The UPS unit shall include Sealed Maintenance Free Lithium Ion Batteries with a typical lifetime of five (5) years and minimum reserve time of four (4) hours under full load conditions. The battery system design shall be provided with necessary devices to prevent deep discharge beyond recommended limits to prevent the batteries discharging beyond end cell voltage specified by the battery maker. The connections from battery to battery shall be by using copper bus bar strips.
TR 7.289	The UPS unit shall provide an output of 230V AC 50 Hz. If the rating of UPS increases above 15KVA at particular location, it should be consider as 3:3 phase UPS and specification should be considered accordingly. If the rating is below 15KVA, it remains as 3:1 phase UPS. The MSI shall be responsible for any conversions needed to support this output configuration.
TR 7.290	The UPS and batteries shall be mounted in a separate cabinet & the enclosure shall be under lock & key, utilising the minimum possible space and arranged in an aesthetic manner.
TR 7.291	The UPS shall be of True online with double conversion topology. It shall support an output power factor at full load as 1.

TR 7.292	The UPS shall have a microprocessor-based unit status and control display with the status and alarm indicators displayed on the status LED indicator and LCD/LED display.
TR 7.293	The UPS unit shall have load level indicators that display the approximate electrical load placed upon the UPS. The UPS unit shall have a row of battery level indicators that display the approximate battery capacity.
TR 7.294	The UPS shall have self-diagnostic functionality to detect any failure/fault in the UPS system and shall display the same on the LCD/LED display of the UPS.
TR 7.295	The UPS unit shall have a minimum of the following LED indicators: • UPS Mode: On-line, Backup/Battery and Bypass; • Over Load Indicator: This will display when UPS is running on overload; • Battery Status Indicator: This will illuminate when battery is low or faulty/disconnected; and • System Fault: This will illuminate when there is some fault or interruption in UPS.
TR 7.296	The UPS unit shall have minimum of the following audible alarms: • Line Failure: This will be audible when required input electrical supply to UPS is not available; • Battery Low: This will be audible when battery voltage falls below the threshold value; • Bypass Mode: This will be audible when UPS is running on bypass mode; and • System Fault: Audible alarm will be generated when any fault is detected in the UPS system.
TR 7.297	The UPS unit shall have following readings on the LCD/LED panel as minimum: • Voltage and frequency Levels: This shall display input and output voltage and frequency levels; • Battery Voltage: This shall display battery voltage in Volts; • Load: This shall display the load connected in percentage to the UPS output; and • Temperature: This shall display the internal temperature of UPS unit for overheating.
TR 7.298	The UPS unit shall include full-time protection from sudden voltage increase with inrush protection and AC line filtering.
TR 7.299	UPS shall provide an overload alarm and circuit breaker designed to operate at an overload of 200% surge.
TR 7.300	The UPS unit shall include Ethernet communication port to support remote management and monitoring capabilities using SNMP including alarm contacts and remote shutdown. Remote monitoring and testing software shall be included. The manufacturer shall provide all SNMP traps.
TR 7.301	The UPS unit shall be capable of starting without input power. The unit shall start up and operate from the battery, with output frequency same as the last operating frequency.
TR 7.302	The UPS unit shall include automatic restart. Upon restoration of utility AC power after complete battery discharge, the UPS shall automatically restart and resume operation.
TR 7.303	The UPS unit shall be enclosed to prevent accidental contact with energized parts.
TR 7.304	The UPS unit shall have a built-in input fuse and/or a circuit breaker for protection from over voltage and current variations.
TR 7.305	The UPS unit shall provide an over voltage shutdown and shall have overvoltage protection.
TR 7.306	The UPS unit shall provide short circuit shutdown protection.
TR 7.307	External battery charger (if required) for the specified battery bank shall be provided. The battery charger shall automatically recharge the battery.
TR 7.308	The external battery charger shall be provisioned to be mounted in the cabinet or UPS itself. Except this, no separate space will be provided for mounting of the external charger.
TR 7.309	The UPS unit shall be compliant to IEC 62040-1 safety standards as a minimum.

TR 7.310	The UPS shall have a BACnet card for integration with BMS.
TR 7.311	The UPS system shall have an operating temperature of 0 degrees to 40 degrees C.
TR 7.312	Any field UPS system (as per MSI's design) shall be supplied with an environmentally rated cabinet for installation of the UPS and batteries. The cabinet shall have a rating of IP 55. The cabinet shall be supplied with in-built fans and proper ventilation as needed to ensure that the temperature inside the cabinet does not exceed 40 degrees C at any given point in time.

2.2.7.6 *Databases*

Any commercially available database like Oracle/Informix/MS SQL /DB2 shall be provided along with license and support and upgrade costs.

Functional Requirements

Databases	
FR 7.5	Database License should be un-restricted and perpetual, to prevent any non-compliance in an event of customization & integration.
FR 7.6	Databases shall support multi hardware platform.
FR 7.7	Database shall provide standard SQL Tool for accessing the database. The tool should be able to monitor, maintain and manage the database instance, objects, and packages.
FR 7.8	Database shall have built-in backup and recovery tool, which can support the online backup.
FR 7.9	Database shall be able to provide database level storage management mechanism, which should enable the availability by means of creating redundancy, automatically balance the data files across the available disks, i/o balancing across the available disks for the database for performance, availability and management.
FR 7.10	Database shall support for central storage of data with multiple instances of database in a clustered environment access the single database/multiple database.
FR 7.11	Should be an enterprise class database with the ability to support connection pooling, load sharing and load balancing when the load on the application increases.
FR 7.12	Database shall provide native functionality to store XML, within the database and support search, query functionalities.
FR 7.13	Database shall have built-in DR solution to replicate the changes happening in the database across DR site with an option to run real-time reports from the DR site without stopping the recovery mechanism.
FR 7.14	Database shall have Active-Passive failover clustering with objectives of scalability and high availability.
FR 7.15	Database shall provide mechanism to recover rows, tables when accidentally deleted. The mechanism should provide ways and means of recovering the database.
FR 7.16	Database shall provide functionality to replicate / propagate the data across different databases.
FR 7.17	Ability to add nodes to cluster with no downtime with-out unloading/reloading data.
FR 7.18	Database should support partitioning feature in table level object.
FR 7.19	Database shall provide native functionality to store XML, Images, Text, Medical Images, CAD images within the database and support search, query functionalities.

FR 7.20	Database shall include tools for enterprise class high availability solution like monitoring performance, diagnose and alert for problems, tuning bottlenecks, resource monitoring and automatic resource allocation capabilities.
FR 7.21	Database must support the SQL queries or latest applicable standard for queries.
FR 7.22	Database shall provide security mechanism at foundation level of the database, so that the options and additions to the database confirm the security policy of the organization without changing the application code. Shall confirm to security evaluations and conformance to common criteria.
FR 7.23	Database shall provide control data access down to the row-level so that multiple users with varying access privileges can share the data within the same physical database.
FR 7.24	Database shall support for enhanced authentication by integrating tokens and biometric technologies.
FR 7.25	Database shall provide functionality for classifying data and mediating access to data based on its classification for multi-level security and mandatory access control, manage access to data on a "need to know" basis.
FR 7.26	Database shall be having native auditing capabilities for the database. Should support optional Audit Capability to store the audit records in separate audit store with monitoring & reporting for multiple databases to detect any security breaches.
FR 7.27	Database shall be having built-in provision to Administer database / database clusters, Monitor performance, Maintain database, Backup and recovery, Recovery management, Disaster recovery management.
FR 7.28	The Management tool should provide advisory-based performance tuning tool which help to tune the queries or objects, SQL analysis, SQL access.
FR 7.29	The enterprise database should provide single web-based console for management of the database.
FR 7.30	Databases shall be as per Bidder’s solution and shall meet RFQ cum RFP requirements.
Restart and Recovery	
FR 7.31	Availability of recovery/restart facilities of the DBMS.
FR 7.32	Automated recovery/restart features provided that do not require programmer involvement or system reruns.
FR 7.33	Program restart should be provided from the point of failure.
FR 7.34	Ability to manage recovery/restart facilities to reduce system overhead.
FR 7.35	Provides extra utilities to back up the databases by faster means than record by record retrieval.
FR 7.36	Provides clear error reporting, recovery and logging.
FR 7.37	Describe recovery strategies that needs to be in place.
FR 7.38	System should support mirroring for DRP.
Backup Procedures	
FR 7.39	Describe Backup Procedures you plan to deploy.
FR 7.40	Describe backup application(s) your proposed solution use.
FR 7.41	Provide details of data backup and restore processes and procedures for all data elements.
FR 7.42	Provide details of automated archiving procedures to copy active data to storage media when archive 'age' is reached.
Error Handling	
FR 7.43	Ability to trap a transaction failure through: • Application Software

	• DBMS • Availability of manual containing all system error messages and correction procedures
System Control	
FR 7.44	Provide details of the 'Audit trail' facility for your proposed solution.
FR 7.45	Should provide adequate auditing trail facility.
FR 7.46	System should record the date and time stamp for all records.
FR 7.47	Ability to track terminals from where the system is accessed.

2.2.7.7 Hardware Security Module (HSM)

Technical Requirements

TR 7.313	The HSM module shall provide a safeguard for digital signatures, cryptographic key storage, transactional acceleration, certificate signing, code signing, bulk key generation, data encryption, DNSSEC.
TR 7.314	The HSM module shall communicate through Ethernet ports.
TR 7.315	A single HSM module shall be separated into different isolated partitions, with each partition functioning as an independent HSM.
TR 7.316	Each independent partition shall support a minimum of 100 cryptographically Partitions / Virtual HSM in order to store different signatures/ certificates in each partition.
TR 7.317	The HSM module shall provide end-to-end integration with various Security Information and Event Management (SIEM) platforms.
TR 7.318	The HSM software shall have an industry-standard professional-grade licensed version of Windows, Linux, Solaris, AIX, HP-UX based OS.
TR 7.319	The systems shall be capable of minimum of 1000 RSA Transactions Per Second (TPS).
TR 7.320	It shall also support virtual based operating system like: • VMware • Hyper-V • Xen
TR 7.321	The HSM module shall also support cloud based operating system.
TR 7.322	It shall support various API modules including PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL, REST as a minimum.
TR 7.323	The module shall comply with the following safety and environmental standards: • UL, CSA, CE • FCC, CE • RoHS, WEEE
TR 7.324	It shall support standard 19” rack mount chassis.
TR 7.325	The module shall be powered by 100-240VAC, 50-60 Hz input as per the design requirements with hot swappable dual redundant power supply.
TR 7.326	The module shall support an operating temperature range of 0°C to +35°C with relative humidity of 10-85%, non-condensing.
TR 7.327	The module shall have a Mean Time Between Failure (MTBF) of at least 50,000 hours.

2.2.8 Streetlight Control System

2.2.8.1 Overview

To control the streetlight infrastructure being planned for implementation across AURIC, the Master Systems Integrator (MSI) shall implement a Streetlight Control System. This shall enable the AITL staff to monitor the status of streetlights.

BR - 8 Business Requirements

BR 8.1	The Streetlight Control System shall enable AITL staff to monitor/control the status of streetlight infrastructure at the group level for AURIC. System shall be implemented specifically for Shendra area. .
BR 8.2	The existing Central Management Software is of Crompton make. It is required to integrate Street Lighting Gateways (SLGs) with existing software. Any additional license(s) for the purpose of integrations or scaling up the application shall be a part of this Project.
BR 8.3	The software application shall enable real-time display of status of streetlights from the AURIC Control Centre (ACC).

FR - 8 Functional Requirements

STREET LIGHTING GATEWAY (SLG)	
FR 8.1	The Street Lighting Gateway (SLG) device shall have the following functionalities: • Server connectivity through Ethernet; • Local On-device storage to bear network outages; • Miniature Circuit Breaker (MCB) trip detection; • Panel door open / closed status detection; and • Manual override activation status detection. • Communications using CCMS on Ethernet (Any converters with last mile communication cable to connect to network switch required shall be provided by MSI)
FR 8.2	The SLG device shall be able to record and transmit values for the following parameters as a minimum through the Energy Meter devices: • Phase-wise voltage; • Phase-wise current; • Power factor; • Active power; • Reactive power; and, • Total Harmonic Distortion (THD).
FR 8.3	The Street Light Gateway (SLG) shall adhere to the below mentioned features as a minimum: • In-built astronomical clock; • Three (3) relay outputs for phase-wise ON/OFF control; • Battery backup to detect and report mains power failure; • Port for interfacing with the Energy Meter device(s);
Electrical Requirements	
FR 8.4	The SLG device shall operate with DC power supply. Any power conversions required shall be provided as part of this Project.

FR 8.5	The SLG device(s) shall have three (3) potential free contacts to deliver the output electricity supply to the streetlights connected with it.
FR 8.6	The electrical setup for Streetlight Infrastructure shall comprise of 20 kVolt surge protection devices per phase as a minimum in between the input power lines and the SLG device.
Environmental Requirements	
FR 8.7	The operating temperatures of Street Light Gateway (SLG) shall be between 0^0C – +55^0C.

2.2.9 Chatbot Solution for Investor Management

AURIC has become a hot-spot of economic activity with various industries and investors expressing their interest for investing in AURIC. In order to assist potential investors, businesses and citizens to invest in AURIC, it is required that the MSI shall enable the interactions between AURIC and investors in a manner as fluid, automated and intuitive as possible. It is also of high value to vibrantly market the state-of-the-art features which are being facilitated to the residents and businesses who would potentially be residing in AURIC. In order to achieve this vision, it is under the MSI's scope to implement a user friendly Investor Management System which shall cater to the needs and queries of investors / businesses / citizens in a 'smart' way for AURIC. The Investor Management System will primarily be a chatbot and shall help in minimizing the in-person interventions and shall also increase the overall efficiency of the system. Here it should be noted that the Chatbot interface shall be developed to cover the investor management services for AURIC which will also include automatic reminders and follow-up with investors and citizens via email.

2.2.9.1 Conceptual Architecture

Chatbot shall have customers which could be citizens, businesses, potential investor which will provide input question or query to the Chatbot in the form of text. Customers shall be able to interact with AITL through different channels. It could be either through the existing social media accounts (Facebook, Twitter etc.) or through the AURIC website and portals launched by AITL. Depending upon the nature of inputs received, MSI shall enable the Chatbot to further categorize them under predefined incident types in the system. This activity shall help the chatbot in prioritizing the inputs and queries. The Chatbot will categorize inputs received and incidents registered under the following categories:

- Transaction issues;
- General Queries;
- Complaints/ grievances;
- Feedback for any AURIC services;
- Incidents related to filing of applications and/or document submission.

It should be noted that the categories mentioned above are tentative only and MSI will be required to add/ modify them post consultation with AITL during the design phase. As per the input or query request, Chatbot layer will prioritize the reply. While some replies would be catered by Chatbot itself, some queries may require immediate intervention by AITL staff for resolution of the same.

Once the queries and/or inputs have been registered and successfully categorized, they interact with the algorithm of Chatbot. And based on the Artificial Intelligence (AI), Machine Learning (ML) and Natural Language Processing (NLP) algorithms, appropriate reply will be provided to the respective customer. The MSI shall ensure that the entire system is developed to be as intuitive as possible.

The Master Systems Integrator (MSI) shall further integrate the Chatbot solution with the existing SAP – ERP platform. Integration of Chatbot and the CRM platform developed by the MSI shall also be done with the existing Smart City Platform operational from the AURIC Control Centre situated at AURIC-Shendra. It shall also enable the AITL to automatically send reminders, alerts and messages via AURIC email ID to investors, businesses and citizens as per defined standard operating procedures.

An example of how the Chatbot will interact with the user has been depicted in Exhibit 9 below.

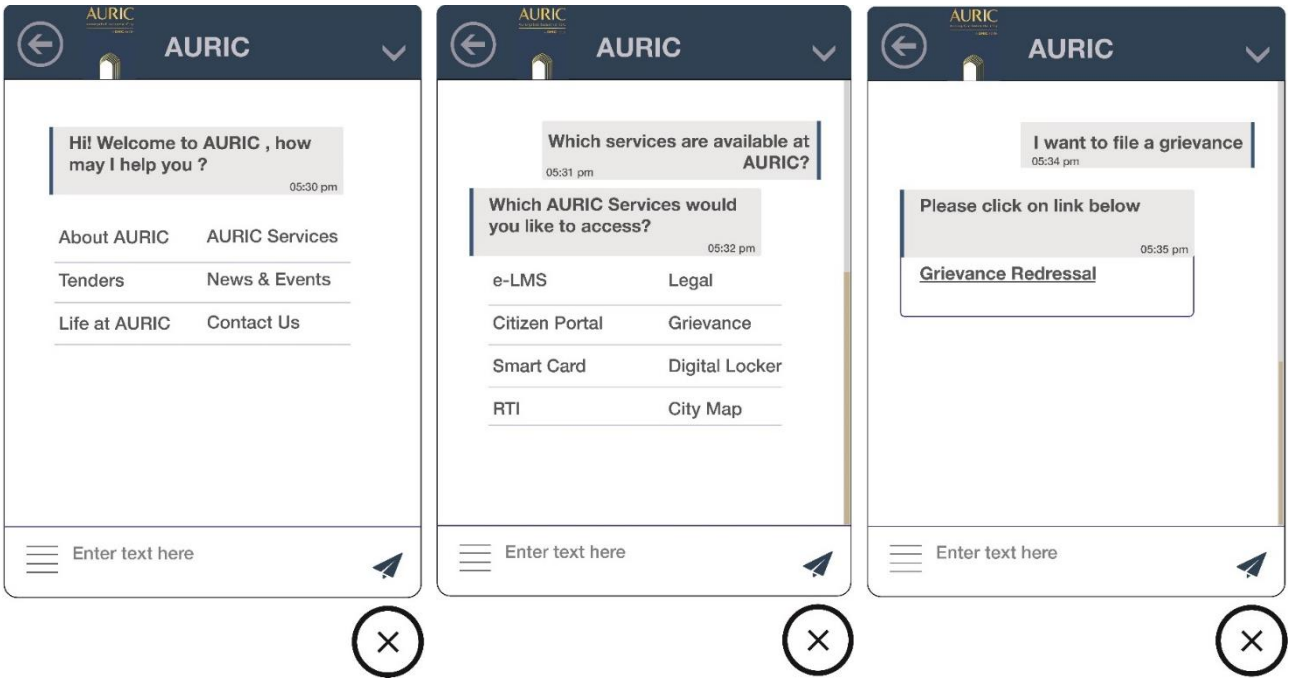


Exhibit 9: Tentative Chatbot user interface illustration

BR - 9 Business Requirements

BR 9.1	The main objectives of the chatbot are as per following: • Address queries of potential investors specific to AURIC; • Ease the land allotment and management process; • Send automatic mails and messages in order to remind and follow-up with investors, citizens and stakeholders regarding necessary actions as per the defined standard operating procedures; • Leverage the data repository to streamline the marketing and outreach process for land allotment; • Assist citizens in availing e-governance services; • Act as a marketing tool; • Enable proactive emergency response management; and • Provide information to city services like maps, events, news etc.
BR 9.2	The Chatbot will use the following channels for interaction: • Corporate website; • Social media accounts like Facebook and Twitter; • AURIC portal; • e-LMS portal; • Mobile application. The above mentioned channels are already existing. The Chatbot solution shall integrate with these channels, which shall be the scope of the MSI.
BR 9.3	Chatbot interface along with Customer Relationship Management (CRM) module shall be implemented for Aurangabad Industrial City (AURIC).
BR 9.4	Chatbot shall have a modular, scalable and reliable architecture to provide quick and accurate responses to the users.
BR 9.5	Chatbot shall have the ability to engage with customers in a user-friendly manner.

BR 9.6	Chatbot shall be able to interact with third party messengers like Facebook Messenger etc. through API(s).
BR 9.7	Chatbot shall be used for offering e-Governance services to the citizens.
BR 9.8	Chatbot shall act as an independent point of contact to AITL officials, citizens and investors.
BR 9.9	Chatbot shall retain all the conversation in order to understand the nature of questions asked by the user so that it can respond accordingly. For this, Chatbot shall utilize the concept of Natural Language Processing (NLP) to learn the kind of queries the users are asking.

FR - 9 Functional Requirements

GENERAL	
FR 9.1	The key elements of Chatbot architecture shall be: • **Front-end interface**: that communicates with the user relying on various messaging channels; • **Natural Language Processing (NLP)**: a component of Artificial Intelligence (AI) which shall form the part of the backend operating algorithm. Having the ability to interpret speech and text as given by users, NLP shall understand, learn and responds accordingly; • **Machine Learning (ML)**: It shall provide machine level logic to train the bot for identifying the nature of speech, sentiments, idioms etc., hence making the bot smart and produce outputs accordingly; • **Database:** Chatbots shall connect to any database at the backend from where it fetches the results to be provided to the user.
FR 9.2	Chatbot shall be operational for 24 x 7 for 365 days a year.
FR 9.3	Chatbot shall be able to maintain a conversation with the user in user-friendly manner.
FR 9.4	The Chatbot shall allow the user(s) to resume their conversation within a predefined time duration.
FR 9.5	The users shall be able to reset their conversation with the Chatbot interface manually.
FR 9.6	Chatbot shall be able to mimic conversation with user in both text or speech formats.
FR 9.7	Chatbot shall respond to the incidents created by it as per the predefined response time.
FR 9.8	Chatbot shall be able to provide correct and accurate results as requested by the user.
FR 9.9	Chatbot shall be attractive, well-designed bot and shall provide text formatting, high-quality links and high-resolution pictures at the time of replying to user.
MACHINE LEARNING	
FR 9.10	Chatbot shall use National Language Processing (NLP) to understand the users' inputs and shall reply accordingly.
FR 9.11	Chatbot shall be integrated with a National Language Processing (NLP) library to minimize the grammatical errors.
FR 9.12	Chatbot shall be able to learn the responses of questions asked by the user in the past, and shall store them for future functioning.
FR 9.13	Chatbot shall inherit its capabilities from Artificial Intelligence (AI) and Cognitive Computing.
FR 9.14	Chatbot shall use a text recognition API to understand the input specified by user.
FR 9.15	Chatbot shall be fed with conversation logs to understand what type of questions require what type of answers.

INTENT DETECTION	
FR 9.16	Chatbot shall assume 'utterance' to be anything received as input from the user.
FR 9.17	Chatbot shall be able to detect user's intent from the utterance received by the user.
FR 9.18	Chatbot shall be able to detect the entity(ies) from the utterance received by the user.
FR 9.19	The Chatbot shall be able to detect user intents programmed manually in the system through machine learning algorithms and AI techniques.
FR 9.20	The AI and Machine Learning algorithms shall enable the Chatbot interface to navigate the user to the appropriate link(s) and/or AURIC services through intent detection mechanisms.
FR 9.21	The Chatbot shall be able to subsequently detect multiple entities in utterances or messages received as input by the user(s).
FR 9.22	The Chatbot interface shall be able to detect the synonyms of entity(ies) input by the user(s).
USER INTERFACE	
FR 9.23	Chatbot shall respond to any input it receives in the following languages as a minimum: • English; • Hindi; • Local language as per Government norms.
FR 9.24	Chatbot shall have improved efficiency with round the clock customer service.
FR 9.25	Chatbot shall be able to reply to the data asked by the user in form of text message.
FR 9.26	Chatbot shall be able to ask for more simplified input, if it doesn't understand the provided input by user.
FR 9.27	Chatbot shall be able to adapt their behaviour based on user interactions.
FR 9.28	Chatbot shall have robust reporting system and dashboard to provide detailed insights of bot's performance.
INVESTOR MANAGEMENT	
FR 9.29	Chatbot interface shall be enabled to publicize AURIC's features and services to investors and citizens.
FR 9.30	Investors and Citizens shall be able to interact with the Chatbot solution through the following social media channels as a minimum: • Facebook; and • Twitter
FR 9.31	Investors and Citizens shall be able to interact with the Chatbot solution through the following AURIC's platforms as a minimum: • Website; • Mobile App; • Land management system platform; and, • Grievance platform.
FR 9.32	The Chatbot shall be able to categorize the user messages into the following categories as a minimum: • Transaction issues; • FAQs; • Complaints; • Feedback; and, • Application filing.

FR 9.33	Chatbot shall be able to respond to users within the predefined response time duration.
FR 9.34	Chatbot shall be able to provide direct access links to citizens and investors for selected AURIC services.
FR 9.35	Chatbot shall be able to notify concerned officials for user messages which require human intervention.
FR 9.36	Chatbot shall automatically send email reminders, messages or alerts to investors, businesses and citizens as per priority and functionality decided with the Client.
FR 9.37	Chatbot shall integrate with the e-mail gateway for the purpose of automatic emails to investors, businesses and citizens.
CUSTOMER RELATIONSHIP MANAGEMENT (CRM)	
General	
FR 9.38	The CRM platform shall be customized in order to ensure seamless flow of operations across the system.
FR 9.39	The CRM shall be able to gather information from all the different channels on which the Chatbot has been interfaced.
FR 9.40	The CRM shall be able to respond to all the identified incidents, requests and queries within a predefined time period.
FR 9.41	The CRM shall enable the Chatbot to provide the best possible answer to the user(s) interacting through the Chatbot interface.
FR 9.42	The CRM platform shall be scalable in nature to incorporate future add-on services in line with established industry standards.
User Interface	
FR 9.43	The CRM shall enable Admin staff to control access to ticket information by other AITL officials.
FR 9.44	The CRM platform shall enable authorized AITL officials to add/ delete/ update the query (ies) and response(s) as per the conversation log between the user(s) and the Chatbot interface.
FR 9.45	The CRM platform shall enable the Chatbot to provide customized responses depending upon the channel of conversation with the user(s).
Ticket Generation & Management	
FR 9.46	The CRM shall be able to generate tickets against any incident, requests and queries received from the user(s).
FR 9.47	The CRM shall be able to route the tickets generated through Chatbot interface to the concerned AITL officials immediately after its generation.
FR 9.48	The CRM shall be able to update the status of tickets on a periodic basis.
FR 9.49	Chatbot user(s) shall be able to check the status of their ticket(s) as and when they wish to do so.
FR 9.50	The CRM platform shall have the capability to auto-escalate any ticket(s) which stand open post the predefined resolution time. The CRM shall also be able to notify the Admin staff about the status of ticket(s) on a periodic basis.
Reporting & Analytics	
FR 9.51	The CRM shall have report generation and analytics capabilities.
FR 9.52	A real-time dashboard for CRM shall enable AITL officials to monitor, address and control the Chatbot input message(s) and communication channel(s) in order to develop a holistic investor management system.

FR 9.53	The real-time dashboard shall enable AITL officials to analyze the efficiency of Chatbot module for investor management.
FR 9.54	AITL officials shall be enabled to filter out the attributes prior to generating reports and analytics (predictive and prescriptive).
FR 9.55	The CRM platform shall enable generation and export of reports in Word, Excel, PDF and CSV formats as a minimum.
INTEGRATION	
FR 9.56	Chatbot shall help users guide to following portals/ websites as a minimum: • Website; • City Services Portal; • Land management system platform; • Grievance redressal platform; and, • City GIS.
FR 9.57	Chatbot shall be integrated to various social media sites like Facebook, Twitter etc. as a minimum.
FR 9.58	Overall Chatbot module shall be integrated with the existing SAP platform so as to interface with the existing ERP platform.
FR 9.59	The existing Smart City Platform shall be able to visualize the analytics generated as part of the CRM dashboard through required API integration.
FR 9.60	Chatbot shall integrate with e-mail gateways for automatic email generation.

2.2.10 AURIC-Bidkin Mini Control Centre (MCC)

As part of the AURIC Smart City Project, it is envisaged that AURIC Control Centre (ACC) at AURIC Hall Building in Shendra will act as the 'nerve' of AURIC that will help in making the city operations, for both Shendra and Bidkin, intelligent, integrated and efficient. Through a centrally integrated platform at the Control Centre, AITL will have capabilities for visualization and analytics of city operations (using Big Data, predictive and prescriptive analytics etc.) via cross-system integration of various systems. All city infrastructure and systems deployed as part of AURIC (Shendra and Bidkin) will be integrated at ACC for central monitoring, control and integrated operations. An essential feature of the ACC is a smart city platform which is a combination of system layers that when combined make use of Big Data, ICT and other infrastructure, advanced computing, analytics, and visualization to enhance a city's intelligence while normalizing the data. As part of Smart City Platform, Cisco Kinetic for Cities (CKC) is being implemented at ACC while SAS platform is being implemented to perform big data analytics. Smart City Platform at ACC will be common for both, Shendra and Bidkin.

As part of Bidkin, it is envisaged that a Mini Control Centre (MCC) will be implemented at the Primary Point of Presence (PoP) site. Bidkin MCC will be a miniature unit of the ACC where monitoring and control of Bidkin applications and its subsequent integration with ACC will take place. Standalone Bidkin applications such as Wi-Fi Management System etc. will be integrated at MCC. Smart City Platform will also be viewed at MCC for monitoring and control purposes. Primary monitoring and control of all Bidkin related applications will take place at ACC only, but monitoring and control feed for standalone Bidkin applications through the smart city platform of ACC will also be enabled at MCC in order to improve operational efficiencies due to geographical constraints.

Depending on the applications, they will be monitored, controlled and integrated with the Smart City Platform at ACC. Overview of the parameters of these Bidkin specific applications is provided below:

SYSTEM	MONITOR	CONTROL	INTEGRATION WITH ACC
Electrical system including metering	✓	✓	✓
Street lighting	✓	✓	✓
Water (including metering) and Wastewater	✓	✓	✓
Environmental Sensors	✓	✓	✓
City Surveillance including ATCC and ANPR	✓	✓	✓
Emergency Communications		✓	✓
Fire	✓		✓
Vehicle Location of AURIC vehicles	✓		✓
ICT infrastructure – Wired & Wireless	✓	✓	✓
Facilities management – AITL building	✓	✓	✓
Facilities management – non AITL building	✓		✓
Transit & Traffic Management (Future)	✓	✓	✓
Education	✓		✓
Healthcare	✓		✓
Multi-Service Digital Kiosks	✓	✓	✓
GIS System	✓	✓	✓
Chatbot for Investor Management	✓	✓	✓

A high level architecture of the Project specifically for interaction with the MCC and ACC is presented as part of Exhibit 10 below.

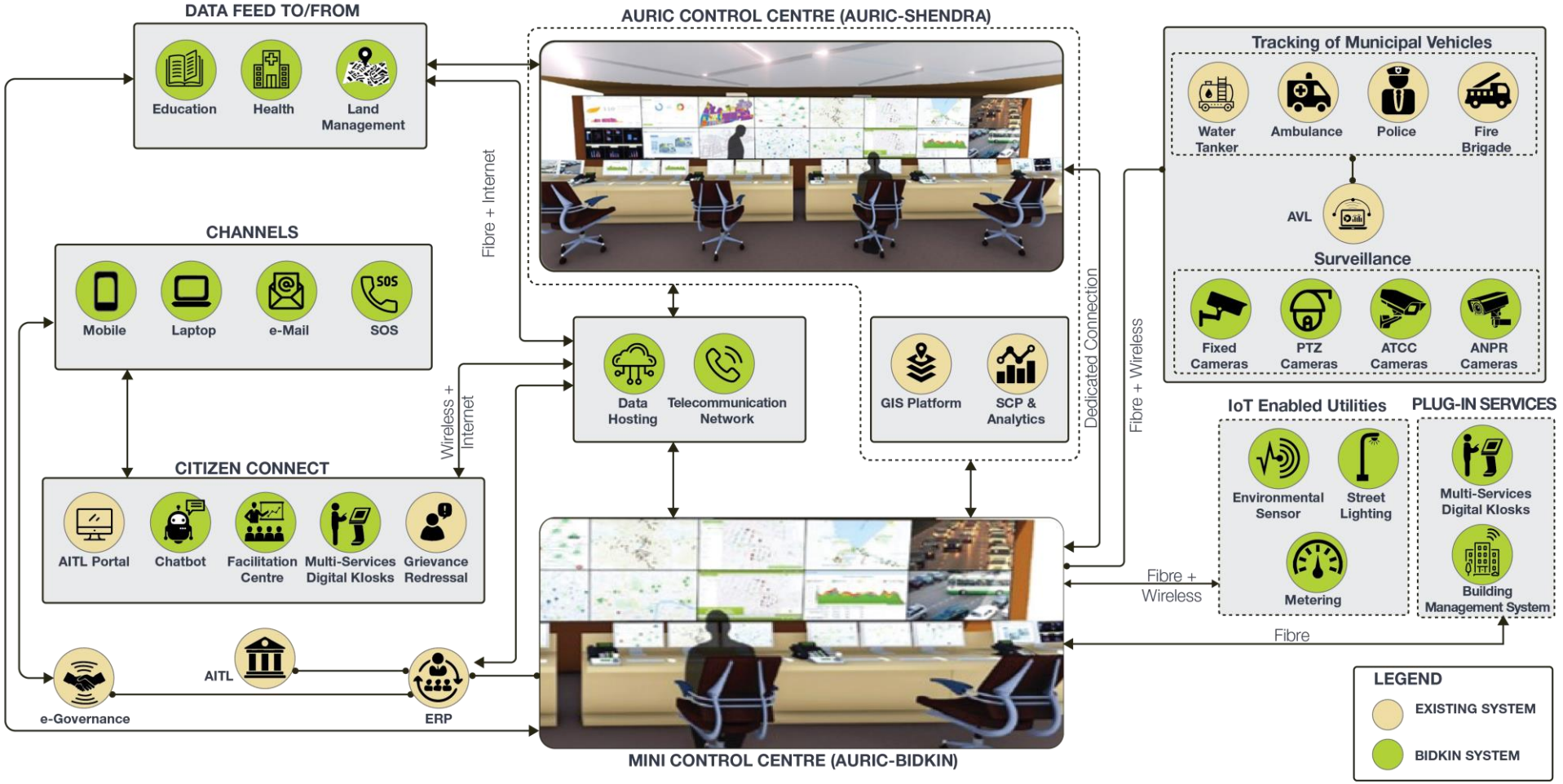


Exhibit 10: High-level architecture for AURIC-Bidkin Phase-1

Exhibit 11 below presents an indicative functional diagram of the logical connections between various components at the MCC. A brief description of each component is presented below.

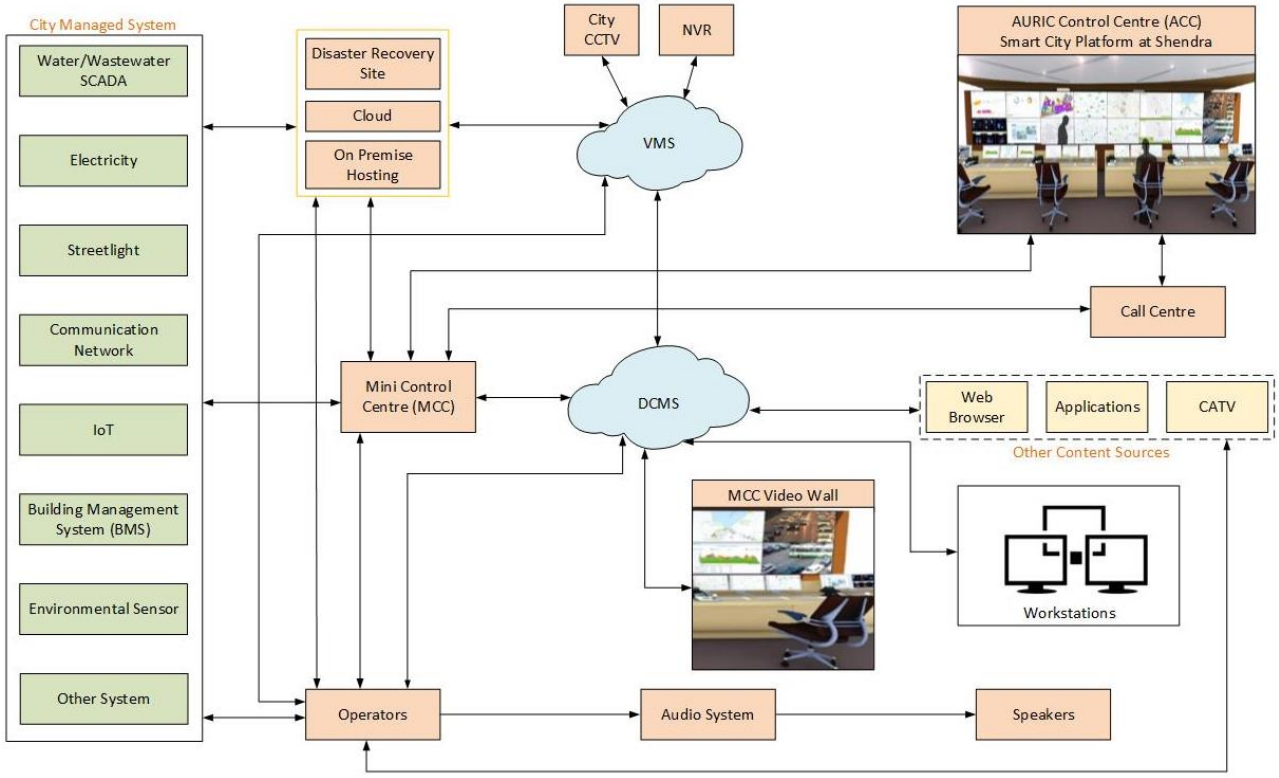


Exhibit 11: Functional diagram of the MCC

- Applications and Web Browsers – Multiple software applications shall be a content input into the MCC Systems.
- Audio System and Speakers – A system of audio components to provide annunciations in the operation spaces within the MCC.
- Call Centre – A 24 x 7 call centre shall be setup to support city operations. The call centre at MCC shall primarily be an extension to the primary call centre at ACC.
- City CCTV Cameras, ATCC and ANPR – These are the primary video inputs into the Video Systems.
- City Managed Systems – Content for a number of city systems to be managed and monitored at the MCC.
- Cloud, Disaster Recovery Site and On-Premise Hosting – Are external to the City limits and used for system applications and data storage for some of the systems.
- DCMS – The Display Content Management System shall manage all networked visual content throughout the facility, including the video display wall and the boardroom display. This system will manage a dashboard for City Management Systems to be displayed and monitored on the video wall.
- Video Recording – Video recorders shall be dedicated for recording and archiving of camera video.
- Operator Workstations – These workstations shall be dedicated for MCC System use at the operator consoles. They are the point of control for the various systems at the MCC.
- Smart City Platform – Various smart city dashboards, Key Performance Indicators (KPI's), and analytics that are available as display visuals to aid city operations and better manage the City. This platform will also input and output feeds from other systems and agencies such as fire, education, healthcare, etc. Smart City Platform will be located at the ACC and all Bidkin systems will be integrated with ACC via MCC.
- Video Display Wall – The Video Display Wall shall be located in the Operations Room and shall be the primary visual display for operators at the MCC.
- Video Management System – The Video Management System shall manage CCTV streaming video, PTZ control, and video archiving.

BR - 10 Business Requirements

BR 10.1	MCC shall act as the monitoring unit for Bidkin and shall assist AITL in enhancing efficiencies of city operations and management.
BR 10.2	MCC shall include a miniature command and control centre, along with workstations and a dedicated rack room.
BR 10.3	MCC shall aggregate all applications specific to Bidkin and shall enable cross-system and cross-agency coordination to monitor, operate and manage the city in an integrated manner.
BR 10.4	MCC shall be integrated with smart city platform at ACC. Using the smart city platform, different agencies/departments of AITL shall be able to monitor and utilize information of other departments for delivering services in an integrated and more efficient manner.
BR 10.5	Smart City Platform feed at ACC shall also be viewed at MCC for monitoring and control purposes for Bidkin specific applications.
BR 10.6	All Bidkin specific developments, integrations and customizations at the smart city platform shall also be catered as part of this project.
BR 10.7	All systems being implemented as part of this Project and Systems provided by 'Other Parties' shall be monitored and controlled on a standalone basis at MCC and further integrated at the ACC as per the requirements of the Project.
BR 10.8	With the data shared through MCC to the smart city platform, AITL shall have capabilities for various visualization and analytics of city operations. These analytics shall be achieved via cross-system integration of various systems and as per the standard operating procedure discussed and agreed upon with the Client. Analytics shall include both prescriptive and predictive analytics.
BR 10.9	MCC shall provide reporting capabilities for city administrators to keep record of city operations.
BR 10.10	The systems at MCC shall ensure that integrity and confidentiality of all information gained is secure at all times.
BR 10.11	The MCC shall be rated for 24x7 operations.
BR 10.12	MCC shall have shift based operations for an overall 24x7 support.
BR 10.13	Integrate all systems from MCC to a central GIS platform implemented as part of Shendra Smart City.
BR 10.14	Smart city platform at ACC will not necessarily duplicate all functionality derived out of individual system specific applications at MCC but will monitor and integrate various features using which an intelligent city operations can be achieved. The monitoring, control and viewing policies will be developed for Bidkin systems and integration capabilities with ACC in consultation with all stakeholders involved.
BR 10.15	ACC will be common for both Shendra and Bidkin. ACC at Shendra has been designed in such a way that it shall be scalable to accommodate future growth and support hardware and software additions and upgrades. In order to achieve this, additional 50% spare capacity for future integrations was kept at ACC. The spare capacity will be leveraged in order to facilitate smooth integration of all Bidkin MCC systems. Any additional hardware requirement on account on integration of Bidkin applications at the Smart City Platform in terms of compute or storage shall be catered through this Project.
BR 10.16	The overall work shall be in reference to standards published as per ISO 37120 and World Council of City Data (WCCD).
BR 10.17	As part of Smart City Platform, Cisco Kinetic for Cities (CKC) is being implemented at ACC while SAS platform is being implemented to perform data analytics. All Bidkin specific integrations shall be done with the aforementioned platforms.

FR - 10 Functional Requirements

FR 10.1	MCC shall provide a holistic and real time view of all city operations on a video wall along with individual views on operator workstations.
FR 10.2	MCC shall enable monitoring, control and automation of various city operations in order to ease and organise city operations.
FR 10.3	MCC shall provide feed of all systems to ACC in order to enable cross system analytics through smart city platform to make city operations intelligent.
FR 10.4	MCC shall leverage information provided by multiple city systems in order to provide an integrated, seamless, proactive and comprehensive response mechanism for day-to-day city operations and challenges.
FR 10.5	Operators at MCC shall be able to view real time dashboards, visualizations, KPIs, historical trending, analytics and other intelligent features through integration with ACC.
FR 10.6	The Digital Content Management System (DCMS), provided as part of MCC, shall manage and drive all visual content to the various display devices, including the video display wall. All city systems will display content through the DCMS.
FR 10.7	All workstation units of the operator workstations shall be installed at the central rack rooms so that space at the MCC operator desks can be optimized. The operators and other personnel operating from the MCC shall only have displays, keyboard and mouse at their workstation desks.
FR 10.8	The operators at MCC shall receive feeds and raw data from the Bidkin City Systems. City Systems shall include the following: • Education • e-Governance and ERP (from ACC) related to Bidkin • Emergency • Healthcare • Power & Water IoT/SCADA • Smart Solid Waste (future) • Street Lights • Environmental Sensors • Surveillance • Telecommunication Network • IoT • Automatic Vehicle Location (AVL) System • Chatbot for Investor Management Any other system being provided as part of this Project.
FR 10.9	Direct connections and data from devices / systems shall include real-time City Systems data, KPIs and video feeds from CCTV cameras.
INTEGRATION WITH SMART CITY PLATFORM AT ACC	
FR 10.10	Smart city platform shall also be viewed at MCC for Bidkin related monitoring and control.
FR 10.11	Data in the form of open protocols shall be shared with ACC from MCC in order to facilitate integrations with smart city platform
FR 10.12	The monitoring, control and viewing policies will be developed for Bidkin systems and integration capabilities with ACC in consultation with all stakeholders involved.
FR 10.13	All customizations, development and integrations on the smart city platform required as part of Bidkin applications shall be also done by the MSI in consultations with the Client.
WATER AND WASTEWATER	

FR 10.14	Communicate locations of personnel, equipment, outage information and safety measures with internal and field personnel.
FR 10.15	Communicate member requests with appropriate internal and field personnel.
FR 10.16	Perform IoT operations as required by line personnel.
FR 10.17	Administer IoT programming and data collection functions.
FR 10.18	Utilize the IoT system to monitor system statistics.
FR 10.19	Dispatch water and wastewater service requests to the appropriate internal and field personnel using the ERP system.
FR 10.20	Provide distribution automation programming support as needed.
FR 10.21	Assist in gathering information for reporting needs (broad reports, departmental benchmarks, etc.)
FR 10.22	Track progress of water and wastewater service requests against pre-determined KPIs.
FR 10.23	Report back to client and contract staff on progress of each water and wastewater service request and close out service requests when completed using the ERP system.
FR 10.24	Maintain asset information held in the database using GIS and ERP system.
FR 10.25	Monitor trunk infrastructure in terms of leaks, breaks, etc.
FR 10.26	Update site specific water and wastewater files and other documentation for helpdesk compliance.
FR 10.27	Billing for services using the ERP system.
FACILITIES MANAGEMENT AND BUILDING MANAGEMENT SYSTEM	
FR 10.28	Interface with the Building Management Systems (BMS) installed at PoPs and other key AITL buildings for monitoring and control of all the building systems and parameters available through the BMS.
FR 10.29	Interface with all the Building Management Systems (BMS) or IP enabled fire alarm system installed in non-AITL buildings for monitoring of essential parameters. A tentative count of 100 non-AITL buildings will be integrated in consultations with the Client.
FR 10.30	Raise an alarm in case a fire alarm is generated from an AITL or a non-AITL building via integration with BMS or fire alarm system. Alerts shall be generated to the emergency authorities and the emergency vehicles from the smart city platform in such a scenario.
FR 10.31	Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person).
FR 10.32	Allocate and dispatch work orders to directly employed (or subcontracted) maintenance team.
FR 10.33	Take ownership of the preventative maintenance (PM) schedule and track reactive maintenance (RM) service requests using the ERP system.
FR 10.34	Track progress of PM and RM service requests against pre-determined KPIs.
FR 10.35	Report back to client and contract staff on progress of each PM and RM service request and close out service requests when completed using the ERP system.
FR 10.36	Maintain asset information held in the database using the ERP system.
FR 10.37	Update site specific facilities management files and other documentation for helpdesk compliance.
FR 10.38	Dispatch of emergency services.
FR 10.39	Create awareness within the city for energy consumption and utilization via information received from smart meters and other SCADA based trunk infrastructure.

POWER NETWORK	
FR 10.40	Monitoring of smart power meters for various parameters.
FR 10.41	Monitor trunk infrastructure in terms of outages, leaks, etc.
FR 10.42	Monitoring of outage or tampering alerts for smart power meters.
FR 10.43	Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person).
FR 10.44	Dispatch outage and power quality calls to the appropriate internal and field personnel using the ERP system.
FR 10.45	Track progress of outage and power quality service requests against pre-determined KPIs.
FR 10.46	Report back to client and contract staff on progress of each outage and power quality service request and close out service requests when completed using the ERP system.
FR 10.47	Maintain asset information held in the database using the ERP system.
FR 10.48	Update site specific power files and other documentation for helpdesk compliance.
FR 10.49	Billings using the ERP system.
FR 10.50	Create awareness within the city for energy consumption and utilization.
COMMUNICATIONS NETWORK	
FR 10.51	Monitoring of the smart telecommunications management system for issues and outages (including any alarms) in terms of passive infrastructure for non-AITL and both active and passive infrastructure for AITL.
FR 10.52	Monitoring and control of the city Wi-Fi infrastructure.
FR 10.53	Monitoring and control of all actives implemented as part of the AITL infrastructure.
FR 10.54	Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person) using the ERP system.
FR 10.55	Dispatch telecommunications service request calls to the appropriate internal and field personnel using the ERP system.
FR 10.56	Track progress of telecommunications service requests against pre-determined KPIs.
FR 10.57	Report back to client and contract staff on progress of each telecommunications service request and close out service requests when completed using the ERP system.
FR 10.58	Maintain asset information held in the helpdesk database using the ERP system.
FR 10.59	Update site specific telecommunications files and other documentation for helpdesk compliance.
FR 10.60	Billings and collections from telecom service providers for revenue sharing using the ERP system.
CITY SECURITY	
FR 10.61	Accurately and promptly observe, monitor and operate closed circuit television (CCTV) cameras and related equipment, and, where necessary direct Police Officers to real time incidents.
FR 10.62	To identify, report, and record anything suspicious, in line with identified procedures.
FR 10.63	To operate surveillance equipment ethically and in accordance with training, policy and procedures, manufacturer's instructions and relevant legislation.
FR 10.64	To ensure all equipment is functioning correctly, carry out equipment checks as required and report all faults to relevant personnel, carry out basic non-technical system maintenance as required.

e-GOVERNANCE & ERP	
FR 10.65	Monitoring of the status of e-Governance systems located at various Multi-Services Digital Kiosks /sites throughout AURIC as well as through the online system.
FR 10.66	Integrate with citizen card via both QR code generation and reading system.
FR 10.67	Log calls/jobs on the helpdesk database utilizing helpdesk software (inquiries may be received by telephone, facsimile, email or in person) using the ERP system.
FR 10.68	Dispatch e-Governance Multi-Services Digital Kiosks /site service request calls to the appropriate internal and field personnel.
FR 10.69	Track progress of e-Governance Multi-Services Digital Kiosks /site service requests against pre-determined KPIs.
FR 10.70	Report back to client and contract staff on progress of each e-Governance Multi-Services Digital Kiosks/site service request and close out service requests when completed using the ERP system.
FR 10.71	Maintain asset information held in the helpdesk database using the ERP system.
FR 10.72	Update site specific e-Governance Multi-Services Digital Kiosks/site files and other documentation for helpdesk compliance.
FR 10.73	Monitor key performance indicators for ERP system in terms of billing, finance, HR, procurement and other modules.
STREET LIGHTING	
FR 10.74	Monitoring of circuits, central control and automation while integrating with the street lighting system.
FR 10.75	Log calls/jobs on the helpdesk database utilizing helpdesk software (inquires may be received by telephone, facsimile, email or in person) using the ERP system.
FR 10.76	Dispatch staff for service request calls using the ERP system.
FR 10.77	Maintain asset information using the ERP system.
ENVIRONMENTAL SENSORS	
FR 10.78	Monitor key inputs from pollution sensors, noise sensors, particle sensors, etc.
FR 10.79	Create awareness within the city based on dynamic inputs received from sensors and display output to various interfaces including city application, multi-services digital kiosks and digital screen.
FR 10.80	Inputs to various regulations and permissions as needed in terms of carbon content, and content of other particles and gases in around Bidkin.
MULTI-SERVICES DIGITAL KIOSKS AND EMERGENCY COMMUNICATIONS	
FR 10.81	Interface with emergency communication modules in multi-services digital kiosks for monitoring and action on emergencies reported by citizens.
FR 10.82	Interface with police, fire and ambulance as needed for emergency services.
FR 10.83	Real-time monitoring of emergency dispatch vehicles.
FR 10.84	Receives and evaluates calls, emails, and online form submissions from internal and external customers requesting information on City services, procedures, activities, resources, and programs in support of the 24-hours-per-day/7-days-per-week; provide information and assistance in an efficient manner.
FR 10.85	Assesses nature or urgency of the issue; determines and establishes priority of call; resolves the issue or escalates and/or transfers call to appropriate staff/agency as necessary.
FR 10.86	Identifies the type of service being requested by listening, asking relevant questions, evaluating information obtained, and determining City services available to successfully handle the request.

FR 10.87	Creates or researches customer information in the Customer Relationship Management (CRM) system; records information on all customer inquiries or problems; provides updates on previously created cases.
FR 10.88	Follows system and department-specific procedures to create service requests and work orders in specialized department software systems.
FR 10.89	Conducts research using various City and public resources to provide customers with complete, accurate, and thorough answers to requests for information, inquiries, and/or problems.
FR 10.90	Dispatches calls in accordance with established procedures and policies using a computerized dispatch system, including determining priority of calls and contacting and sending appropriate response unit.
FR 10.91	Observes and complies with departmental policies and procedures, customer service quality standards, and compliance guidelines.
EDUCATION	
FR 10.92	Monitor key ratios (KPIs) that will be important inputs for economic indicators.
FR 10.93	Monitor any bus-level infrastructure like CCTV, and location of buses as required.
HEALTHCARE	
FR 10.94	Monitor key ratios (KPIs) that will be important inputs for economic indicators.
FR 10.95	Monitor location of ambulances by obtaining feeds from the healthcare facility owners.
VIDEO DISPLAY WALL	
FR 10.96	Video display wall content will not be switched frequently and shall be displayed real-time. It shall be rated for 24x7 operations.
FR 10.97	Functionality of centre zone for common viewing, for example map of the city can be enlarged and copied to the centre of the display wall for general reference.
FR 10.98	Option to create multiple layouts shall be present.
FR 10.99	Video display wall shall be integrated with Display Content Management System (DCMS) so content managed in the DCMS can be displayed on the video wall.
FR 10.100	Ability for all CCTV video, CATV, web pages, IoT and all other display content to be routed to the board room.
FR 10.101	Ability to manage the content within the boardroom or at the operators' consoles.
FR 10.102	Ability to add content from an MCC workstation.
FR 10.103	The video display wall product selected shall be durable for optimal use in a 24/7 operational mode.
FR 10.104	The focus of the design characteristics are ergonomics for the various viewers, quality and stability of the images, uniformity across the whole area, availability of the system, limited maintenance and low disruption of the control room operations.
FR 10.105	Video display wall shall be capable of displaying High Definition (HD) content.
FR 10.106	Gaps between screens shall be negligible to view HD graphics on multi screens.
FR 10.107	Auto calibration feature shall be provided to avoid periodic maintenance. Auto colour and brightness management mechanism shall also be acceptable.
FR 10.108	There shall be a user interface for all settings and operational parameters.

TR - 10 Technical Requirement

VIDEO DISPLAY WALL (VDW)	
TR 10.1	The VDW shall be made up of DLP™ rear-projection cubes. Each DLP™ display cube shall measure 70 inches in diagonal. It shall include all controllers required for its operations.
TR 10.2	The native resolution of each Visual Display Unit / Rear Projection Module should be 1920 X 1080 pixels (Full HD) and should have Laser as its light source with ultra-thin configuration.
TR 10.3	The light source lifetime of the laser shall be at least 100,000 hours.
TR 10.4	The brightness uniformity of the VDM shall be >95%.
TR 10.5	The project engine of VDW shall be rated for performance in project conditions.
TR 10.6	The Rear Projection Module shall have laser as its light source.
TR 10.7	The screen shall have negligible inter screen gap to give seamless viewing experience.
TR 10.8	The Cube shall have inbuilt redundancy in power supply and laser light source.
TR 10.9	The dashboard shall be capable of simultaneously displaying one (1) to one hundred (100) independent sets of information on the video display wall. Specific outputs to be displayed shall be chosen by operators.
TR 10.10	The VDW shall include video walls mounted close to each other to give a seamless viewing experience.
TR 10.11	Each cube of the VDW shall have its own IP address and on-board web server to provide standard information like status and health.
TR 10.12	The VDW shall be the primary visual information point to see CCTV videos, incident alarms, IoT screens, network health conditions, GIS maps, and any application running on city systems.
TR 10.13	The VDW shall provide a collaborative visual for operators and management to work and coordinate on various tasks in different situations.
TR 10.14	The VDW product selected shall be durable for optimal use over a long time in a 24/7 operational mode.
TR 10.15	The VDW shall provide image uniformity across the whole display area.
TR 10.16	The VDW shall have system availability with limited maintenance and low disruption of the operations room operations.
TR 10.17	The VDW shall be capable of displaying high definition (HD) and standard definition (SD) content.
TR 10.18	The VDW shall provide minimum viewing angles of: • Horizontal - ±35 degrees • Vertical - ±27 degrees
TR 10.19	Auto colour and brightness management mechanism to be provided.
TR 10.20	The VDW shall have a user interface for all settings and operational parameters.
TR 10.21	The VDW shall support with enhanced brightness of at least 500 cd/m² to accommodate ambient light expected inside the room.
TR 10.22	The VDW units shall be new and current to the manufacturer's product line. The units shall not be discontinued products.
TR 10.23	Each VDW unit shall have front-access to the projection modules and internal components of the cubes for maintenance purposes.
TR 10.24	The brightness uniformity of each display cube and across the entire VDW shall be at least 95%.

TR 10.25	The video display cubes shall have anti-reflective screens in order to reduce reflection and glare on the display wall.
TR 10.26	The VDW shall not daisy chain video communications from one display cube to another. There shall be a direct video connection from the display content management system to each display cube.
TR 10.27	All video display cubes shall have a consistent image quality and brightness across the display wall.
TR 10.28	The VDW will have at least one (1) female DVI-I/HDMI input connector.
TR 10.29	The VDW shall have 10/100/1000 copper Ethernet communications port.
TR 10.30	A pedestal shall be provided to support the VDW. If the manufacturer's standard pedestal does not comply with the height requirement, the MSI shall supply a custom setup.
TR 10.31	The support structure shall be with a laminate finish.
TR 10.32	The support structure shall have open internal space for equipment.
TR 10.33	The support structure shall have easy to open front access covers.
TR 10.34	The MSI shall provide lateral support for the VDW. If fixations are required behind the VDW, the MSI shall propose and design an appropriate support system.
TR 10.35	The VDW pedestal shall be physically secured to the concrete floor of the building. It shall not sit on top of the raised floor.
TR 10.36	Each VDW projection engine shall be modular having input module and optical engine separate" to introduce more competition.
TR 10.37	The VDW shall allow for easy maintenance of modules, colour sync systems, etc. where downtime is no greater than 60 minutes.
TR 10.38	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz. Power consumption of each cube shall be less than 350W.
TR 10.39	The VDW shall have an operational temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
TR 10.40	The VDW shall have a relative humidity of 20 to 80%, non-condensing or better.
TR 10.41	The VDW shall be of sufficient design, manufacturing and operational quality to provide twenty-four (24) hours, seven (7) days a week mission critical functionality.
TR 10.42	The VDW shall have redundancy of critical components like light module, and power supplies.
Display Content Management System (DCMS) or Video Wall Management System	
TR 10.43	The DCMS shall include the VDW controller for the Operations Room VDW and a system to manage the visual content.
TR 10.44	The DCMS shall be able to display visual content on any network attached display device.
TR 10.45	The DCMS shall be able to input, manage, and distribute visual content.
TR 10.46	The DCMS shall be able to decode, transmit, manage, and display the following formats of digital streaming video: • MPEG-4 • H.264
TR 10.47	The DCMS shall treat the VDW as a single display. It shall act as a single canvas with no pixel separation.
TR 10.48	The DCMS shall have the ability to create multiple spaces for different users to control display content. The DCMS shall be able to create a minimum of six (6) distinct operator controlled display areas. These display areas cannot cross over into another. The display areas can be created anywhere within the VDW.

TR 10.49	The DCMS shall be able to create display layouts for any sized display, including boardroom monitor and the operations room display. The DCMS shall be able to save a minimum of one hundred (100) display layouts for every display device within the MCC.
TR 10.50	The DCMS shall be able to manage users and roles. The DCMS shall have an administrator role to have master control of all functions.
TR 10.51	The DCMS shall be able to separate the video wall into variable sized sections so that system defined users can manage only their portion of the video wall. Users not belonging to a particular group managing another portion of the video wall shall not be entitled to change layouts and sources.
TR 10.52	The DCMS shall be able to stretch, re-position, and resize any video source on any display device.
TR 10.53	The DCMS shall be supplied with a user interface (UI) independent of other systems. Three (3) mouse clicks (average) to execute DCMS function is a requirement for performance.
TR 10.54	The DCMS shall have a seamless interface within the VMS UI of the CCTV.
TR 10.55	The DCMS shall be accessible on any networked workstation or networked monitor with OPS on the MCC network.
TR 10.56	The DCMS shall be able to create and edit user groups. DCMS permissions for users and user groups shall be customizable. At a minimum the definable permissions shall include UI function rights, viewing access rights, source list access rights, and display access rights.
TR 10.57	The DCMS shall include an administrator role that shall be able to manage system configuration, sources, user groups, and user authentication.
TR 10.58	All users on the DCMS shall have a password-protected login.
TR 10.59	The DCMS shall be able to display a minimum of two hundred (200) independent visual sources simultaneously on the VDW in the Operations Room. The sources shall be of HD or 4CIF resolution.
TR 10.60	The DCMS shall be able to display a minimum of twenty (20) independent visual sources simultaneously on all boardroom or auxiliary display device. The sources shall be of 4CIF resolution or HD.
TR 10.61	The DCMS shall be able to add borders to individual original video content source.
TR 10.62	The DCMS shall be able to display a minimum of ten (10) web browser applications without the use of screen capturing from an external network source.
TR 10.63	The DCMS shall be able to select and display any region of a multi-monitor display on a DCMS connected source. For example, if an operator has three (3) monitors, the operator can select monitors one (1) through two (2) for display on the VDW, while leaving monitor 3 for local display only. It is also acceptable that The DCMS be able to select and display any multi-monitor display on a DCMS connected source. For example, if an operator has three (3) monitors, the operator can select monitors one (1) through two (2) for display on the VDW, while leaving monitor 3 for local display only.
TR 10.64	Visual content from networked sources shall be transmitted and displayed with no pixel loss or degradation.
TR 10.65	The DCMS shall be able to accept a minimum input of four (4) CATV video sources. Demodulator shall be a part of the overall MSI solution, if required to comply with the given requirement.
TR 10.66	The DCMS shall be able to search for networked video sources.
TR 10.67	The DCMS shall have the ability to accept and use General Purpose Interface (GPI) triggers from the AITL's systems to activate pre-set image configurations.
TR 10.68	The DCMS workstation client software shall run on an industry standard-based operating system.

TR 10.69	The DCMS shall be able to run a minimum of twenty (20) workstation client software instances simultaneously. DCMS shall be intelligent.
TR 10.70	The DCMS shall have the ability to self-monitor and provide alerts to the administrator and designated users via e-mail.
TR 10.71	The DCMS shall have a SDK and API openly available without charge for future integration with third party applications.
TR 10.72	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 10.73	The DCMS shall support 10/100/1000 Ethernet communications for device management and other communication.
TR 10.74	All DCMS hardware shall have an operational temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
TR 10.75	The DCMS shall have redundancy of critical components to support a twenty-four (24) hours, seven (7) days a week mission critical functionality.
Video Wall Management Software	
TR 10.76	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or schedule/timer based.
TR 10.77	The software should enable the users to see the desktop of the graphics display wall remotely on the any PC or above connected with the DCMS and Video Wall over the Ethernet and change the size and position of the various windows being shown.
TR 10.78	The software should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the DCMS and Video Wall on the Ethernet.
TR 10.79	The software should copy the screen content of the workstation connected on the Ethernet with the DCMS to be shown on the Display wall in scalable and moveable windows in real time environment.
BOARD ROOM MONITOR	
TR 10.80	The display shall utilize LCD with backlit LED technology.
TR 10.81	The display shall be seventy inches (70”) diagonal at minimum.
TR 10.82	The display shall have a native resolution of UHD resolution.
TR 10.83	The display shall have an aspect ratio 16:9.
TR 10.84	The display shall be equipped with a media USB for direct plug and play from USB.
TR 10.85	The display shall have a built-in or external tuner.
TR 10.86	The display shall be a commercial grade product.
TR 10.87	The display shall have a built-in low profile speaker.
TR 10.88	The display shall have a typical brightness greater than 300 cd/m^2.
TR 10.89	The net weight of the display shall be less than 100 Kgs.
TR 10.90	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 10.91	The boardroom monitor shall equipped with at least one (1) of each input format including HDMI, Display Port, and Ethernet (RJ45).
TR 10.92	The boardroom monitor shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
VIDEO CONFERENCING (VC) SYSTEM	
TR 10.93	The VC system shall allow live visual connection between two or more people residing in separate locations for the purpose of communication. The VC system shall be integrated with the EPABX system being provided as part of this project.

TR 10.94	The VC system shall be flexible, provides interactive content collaboration to distant teams.
TR 10.95	The VC system shall support transmission of full-motion video images and high-quality audio between 2 or more locations.
TR 10.96	The VC system shall support multipoint videoconferencing which allows three or more participants to sit in a virtual conference room and communicate to each other.
TR 10.97	The VC system shall have the following capabilities: white boarding, annotating, and application sharing from a computer or tablet. All shall be included as part of a comprehensive, collaborative video session.
TR 10.98	The VC system shall have innovative facial-tracking algorithms/push-to-talk option to accurately frame all room participants.
TR 10.99	The VC system shall support 16:9 and 4:3 aspect ratio, automatic gain control, and intelligent audio mixing.
TR 10.100	The VC system shall support multiple video sources.
TR 10.101	The VC system shall have the capability to zoom in and follow the person speaking.
TR 10.102	The VC system camera shall offer brilliant visual clarity with a HD sensor, and shall be available with 12x zoom and a wide-angle lens adapter.
TR 10.103	Participants shall be able to have the following feature controls using Remote Control or GUI of video system or through the video conferencing MCU: • Mute My Line / Unmute My Line • Increase Broadcast Volume / Decrease Broadcast Volume • Mute All Except Me / Cancel Mute All Except Me • Change Password • Mute Incoming Participants / Unmute Incoming Participants • Play Help Menu • Enable Roll Call / Disable Roll Call • Roll Call Review Names / Roll Call Stop Review Names • Terminate Conference • Start Personal Layout • Change To Chairperson • Increase Listening Volume / Decrease Listening Volume • Override Mute All • Start Recording / Stop Recording / Pause Recording • Secure Conference / Unsecured Conference; and • Show Number of Participants
TR 10.104	The VC system camera shall be mountable on flat panel display or on a shelf in the cart.
TR 10.105	Controls of the VC system shall be accessed via the room control system to maintain a single source for control.
TR 10.106	The VC system shall include a codec, camera, microphone with option to extend additional microphone/s and remote controller for user control.
TR 10.107	The VC system UI shall be intuitive and easy to use.
TR 10.108	The VC system shall support following video standard protocols: • H.261/H.263/H.264 AVC • H.263/H.264 video error concealment

TR 10.109	The VC system shall have at a minimum, the following audio and video inputs; • 2 x camera • 3 x USB Any converters required for video display shall be provided by the MSI.
TR 10.110	The VC system shall have at a minimum, the following other interfaces; • 2 x USB 2.0
TR 10.111	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 10.112	The VC system shall use 1 x 10/100/1000 Ethernet and support IPv4 and IPv6.
TR 10.113	The VC system shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
MONITORS	
TR 10.114	The monitor shall be of LED flat panel screen technology with following size; • 24-inch diagonal • Widescreen format (16:9 aspect ratio) • Thin bezel not exceeding ½ inch • HD 1920x1080 resolution • Minimum input of 1xDP, 1x HDMI, 1xDVI • Energy Saving • Allow tilt and swivel motion • Black colour
TR 10.115	The monitor shall have high refresh rate to eliminate screen flicker causing eyestrain and headache.
TR 10.116	The monitor shall support the same refresh rate as the workstation video card.
TR 10.117	The monitor shall have response time sufficient to limit ghosting in video, in particular on detail video monitor.
TR 10.118	The monitor shall have accurate depiction of colour to enable distinction of colour coding used in display content, and video monitors).
TR 10.119	The monitor shall have highly focused distortion-free images, to enable accurate reading of map detail and distinction of items close to one another on display content.
TR 10.120	The monitor shall have even level of brightness across entire screen.
TR 10.121	The monitor shall have good colour convergence on all points of screens; no bleeding out of colours at the edges of characters.
TR 10.122	The monitor shall have anti-glare screen.
TR 10.123	The monitor shall have adjustment controls (e.g., brightness/contrast) easily accessible, easy to locate and easy to use.
TR 10.124	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 10.125	The monitors shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
TR 10.126	The monitor shall be designed for Designed for 24/7 operations over 5 year period.
CEILING SPEAKERS	
TR 10.127	The ceiling speakers shall have high power and high sensitivity with extended frequency responses.
TR 10.128	The ceiling speakers shall have wide, controlled constant directivity dispersions for optimum coverage.

TR 10.129	The ceiling speakers shall have output of at least 15W peak. They shall have in-built amplifiers or shall be supported by an external amplifier.
TR 10.130	The ceiling speakers shall have a conical coverage pattern of at least 105 degrees (1kHz – 6 kHz).
TR 10.131	The ceiling speakers shall be in a colour to match the ceiling and surrounding interior design.
TR 10.132	The ceiling speaker shall have a diameter not greater than 8.5”.
TR 10.133	MSI shall quantify and space speakers to provide full audio coverage within the operation room and boardroom.
TR 10.134	The ceiling speakers shall follow the manufacturer recommendation for connectivity.
TR 10.135	The Ceiling Speakers shall automatically adjust the output audio level based on ambient noise. This may require either in-built noise sensors with the ceiling speakers or an independent ambient noise monitoring system.
TR 10.136	Any associated component such as audio processors, amplifiers etc. which are required to operate the speakers shall also be included as part of the overall solution.
TR 10.137	The ceiling speakers shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
Operator Console	
Materials	
TR 10.138	Consoles are primarily a workspace that support operator workstations and monitors for monitoring various systems at the MCC, including the independent city systems and smart city platform. They maximize workspace for both the operators and communications staff, while meeting the ergonomic and occupational needs for staff working shift patterns with 24/7 coverage.
TR 10.139	All operator consoles shall be designed to meet the shape, dimensions, and orientation requirements within the Operations Room.
TR 10.140	The consoles shall satisfy the functional, aesthetic and ergonomic requirements of the working environment of the Operations Room staff.
TR 10.141	All console materials and components shall be of sufficient design, manufacturing, and operational quality to provide dependable and durable performance for constant use 24 hours a day, every day of the year.
TR 10.142	The consoles shall provide work surfaces with multiple vertical locations (stand / sit system) - standing height, work surface height, and below work surface height.
TR 10.143	The consoles shall be of a modular design, allowing for future equipment and room layout configurations.
TR 10.144	The consoles shall be fabricated to meet or exceed recognized industry quality standards (e.g., ANSI/BIFMA or equivalent).
TR 10.145	The consoles shall be designed to accommodate a variety of computer displays, communications and operator interface devices and include appropriate power and data cabling management for said devices.
TR 10.146	Each console shall be capable of accommodating, as a minimum: • Operator desk and chair • Three (3) wide-screen 610 mm (24 inch) LED monitors • One (1) standard keyboard • One (1) standard mouse • One (1) set of headset jacks mounted underneath desk

	• One (1) VOIP telephone • One (1) two-way radio (future) • Free space for paperwork • Desk slats for binder/manual storage; and • One (1) large file drawer for storage
TR 10.147	A selection of finishes shall be available for all console components. The console provider shall provide sample finishes to coordinate with the Operations Room environment, millwork, aesthetics, and the adjacent Cabin / Boardroom furniture finishes.
TR 10.148	All console components shall include trim pieces including fillers, connectors, full or partial end trims, top caps, etc. as required to create a professional appearance.
TR 10.149	All consoles and components shall not display manufacturer or vendor logo, name, or equivalent signage and nameplates.
Structure	
TR 10.150	Each console main structure shall be constructed of thick wall custom profile extruded aluminium alloy, or structural equivalent (e.g., 10 gauge steel).
TR 10.151	Structural assembly components (e.g., cabinet frames) shall be constructed of precision-tooled cold-rolled steel, or structural equivalent, and finished with durable electrostatic powder coat finish, or equivalent.
TR 10.152	Levelling glides shall provide a maximum height adjustment of up to 64 mm (2.5 inch) for each console and component.
TR 10.153	Structural assembly components shall be bolted as required to the raised floor tiles through the carpet tiles at locations a minimum of 305 mm (12 inch) from any floor access or other floor service location.
TR 10.154	Consoles shall provide work surface stability at all vertical positions including full height (stand) position, via suitable structural components such as a third leg.
Mounting System	
TR 10.155	Each console shall furnish a mounting system consisting of either a work surface mount (with articulated arm) or slat wall mount (with double pivoting articulating arm).
TR 10.156	Mounting systems shall be available from 174mm to 522mm in height utilizing a vertical stackable option in incremental heights above the console work surface.
TR 10.157	Stacking elements shall be load-bearing on all tiers and shall use like parts as base panels (i.e. skins, electrical, horizontal beams, etc.) to create a professional appearance.
TR 10.158	Mounting systems shall be capable of being equipped with a maximum of three (3) monitor arms at each console. Monitor arms shall be removable and interchangeable with other consoles. Monitor arms shall be easily moveable horizontally across the mounting system if slat wall mount is used.
TR 10.159	Each monitor arm shall be capable of supporting a variety of typical LED monitor sizes and types (including iPads and other types of tablets) weighing up to and including 23 kg (50 lbs).
TR 10.160	Each monitor arm shall have swivel, tilt, and height-adjustable capability with appropriate positive friction or mechanical locking mechanism to maintain the desired positions and orientations. Monitor arms should be single touch adjustable for ease of use.
Wiring and Cabling	
TR 10.161	Special components shall not be required to bring power, data, and communication wiring into consoles.
TR 10.162	The console placements in the Operations Room and dimensions shall be adjusted accordingly to integrate all cabling service entry accesses in the floor.

TR 10.163	Consoles shall not obstruct or interfere with any raised floor access location cabling services or functionality.
TR 10.164	All consoles shall provide suitable provisions to regain reasonable access to each raised floor access location to preserve the ability to install future power/cabling services into the console via cabling service entry accesses in the floor.
TR 10.165	Each console shall provide a built-in cable management system that accommodates two (2) wiring runs, one (1) for power and one (1) for data and communication (e.g., through hollow leg space or other hollow spaces in the structure).
TR 10.166	Cable management system shall provide continuous and appropriate components to protect all cables, including those connected with extension cords, during height adjustable work surface vertical height transitions.
TR 10.167	The cable management system shall provide appropriate access points and continuous cable management throughout the entire console, including but not limited to: • All floor access locations; and • Entire height adjustable work surfaces of each console, including returns
TR 10.168	The cable management system shall be integrated, routed, and accessible to enable easy addition/removal of cables/wires in the future and shall not be interfered when adding or removing stacking elements.
TR 10.169	The cable management system shall have the capability to accommodate vertical cable runs in all stationary components neatly and internally.
TR 10.170	The cable management system in all stationary structures, bases, frames and components shall be capable of maintaining a minimum 51 mm (2 inch) bend radius required for any future cable.
TR 10.171	Power strips shall be durable metal construction or equivalent.
TR 10.172	Power strips shall not incorporate any surge, overload, or power on/off switch.
TR 10.173	Each console shall provide one (1) fully integrated sixteen (16) receptacle power strip mounted horizontally throughout the entire height adjustable work surface frame, accessible from the work surface.
TR 10.174	Each console shall provide two (2) fully integrated four (4) receptacle power strips mounted vertically at each back corner.
TR 10.175	Each console shall be provided with two (2) computer extension cables that shall connect workstations in the Rack Room to I/O endpoints at the consoles in the Operations Room. Extension cables may consist of powered cable extender units. Extension cables shall be a suitable length, fully shielded, and interface with video, mouse, keyboard, speakers, and microphone computer interfaces.
TR 10.176	Each computer extension cable shall provide the following connectors at the workstation end in the Rack Room: • One (1) HD-15/HDMI male video • One (1) USB female keyboard and DVI/HDMI adaptor • One (1) USB female mouse and DVI/HDMI adaptor • Two (2) USB female (spares) • One (1) 3.5 mm male speaker; and • One (1) 3.5 mm male microphone
TR 10.177	Each computer extension cable shall provide the following connectors at the height adjustable work surface end: • One (1) HD-15/HDMI female video • One (1) USB female keyboard and DVI/HDMI adaptor

	• One (1) USB female mouse and DVI/HDMI adaptor • Two (2) USB female (spares) • One (1) 3.5 mm female speaker; and • One (1) 3.5 mm female microphone
TR 10.178	Wiring and cabling details provided in this set of specifications are indicative only. The console provider shall confirm the wiring and cabling details with the AITL or their designate during the detailed design of the consoles.
Height-Adjustable Work Surfaces	
TR 10.179	Each console shall provide height-adjustable work surfaces, enabling Operations Room staff to work from various vertical positions while sitting or standing. Slat walls (if used) shall automatically raise and lower at the same rate and distance as the work surface is raised or lowered.
TR 10.180	Each console's entire work surface shall be fully height-adjustable.
TR 10.181	Each console height adjustment system shall smoothly and evenly lift and lower all work surfaces together and provide the capability to stop at any time to provide a stable and secure work surfaces at any position within the height range of travel.
TR 10.182	The height adjustment system velocity shall be constant and virtually the same rate when lifting and lowering work surfaces.
TR 10.183	Cable management system shall function without requirement for manual alteration, as the work surfaced is height-adjusted. Cables during lift and lowering operation shall be controlled and protected via a suitable mechanism such as a flexible cable chain or equivalent.
TR 10.184	Sufficient space shall be provided between moving and stationary components for safe movement, with no pinch points.
TR 10.185	Each console shall provide reasonable maintenance and service access to height adjustment system electrical and mechanical components.
Desk Binder/Manual Storage	
TR 10.186	Each console shall have one (1) binder/manual storage unit above desk top.
Free Work Space	
TR 10.187	Each console shall have sufficient free work space for paper work on the console desk top.
TR 10.188	Free work space shall be at least 0.61 linear metres (2'-0" linear feet) of the console desktop.
Keyboard Trays	
TR 10.189	Each console shall have an ergonomic keyboard tray drawer installed underneath the desk workspace.
TR 10.190	Ergonomic keyboard tray drawers shall glide on steel ball bearings and shall be mounted with durable metal hardware.
Large File Drawer	
TR 10.191	Each console shall have one (1) large file drawer unit with lockable casters for storage below the desk top, minimum 305 mm (12 inch) high.
TR 10.192	As a minimum, the following drawer fronts construction material shall be available: • 17 mm (11/16 inch) particle board core with high-pressure laminate facing and edges • Steel with powder coated finish; and • Wood veneer with solid wood facing and edges
TR 10.193	Drawer glide shall be a minimum two-part precision steel ball bearing suspension, with cushioned stops, both in and out.

TR 10.194	File drawer is to expose a minimum of 100% of its overall length when fully extended from the console.
TR 10.195	File drawer shall have drawer bumpers to cushion and quiet the drawer.
TR 10.196	Drawer dividers and one (1) pencil tray shall be included in the file drawer. The pencil tray should be about 102 mm (4 inch) wide and 25 mm (1 inch) deep, and the length of the pencil tray shall be equal to the width of the drawer. The pencil tray shall be secured in the drawer in such manner to prevent its sliding during the operation of the drawer.
TR 10.197	File drawer shall be provided with compressor/hanging rails for side-to-side filing.
TR 10.198	File drawer shall accommodate legal and letter paper filing.
Reliability	
TR 10.199	Consoles shall be designed for high durability and performance.
TR 10.200	Consoles shall be warranted for 24/7 use.
Operator Workstations	
TR 10.201	The workstations shall be rack mounted with only keyboard, video, and mouse at the operator console. The MSI shall neatly install the workstations at the designated rack locations in the rack room.
TR 10.202	Please refer to the Workstation Specification as mentioned under IT Infrastructure specification Section 2.2.7.2 for other details on the workstations.
Laptops	
TR 10.203	Please refer to the Laptop Specification as mentioned under IT Infrastructure specification Section 2.2.7.2
Task Lights	
TR 10.204	Task lights shall maintain the required lux level (400-500 lux).
TR 10.205	The task lights shall have a professional appearance and ergonomic design to complement the console and Operations Room and Cabin / Boardroom aesthetics.
TR 10.206	Task lights cords shall be non-handed.
TR 10.207	Task lights reflector shade shall be designed to provide a glare-free lighting on work surfaces.
TR 10.208	Task lights shall be provided with a weighted base providing a minimum 340° arm rotation.
TR 10.209	The task light on/off switch shall be located in the front of the light for easy accessibility.
TR 10.210	All task lights shall use LED or low voltage lamps. Each task light shall be provided with two (2) suitable lamps. One (1) shall be installed for immediate use and one (1) shall be delivered to the MCC as a spare.
Multi-Functional Printers including Scanner	
TR 10.211	Printers shall be of latest laser technology & for duplex printing (colour and black and white) for all paper size including but not limited to A4 and A3.
TR 10.212	It shall have Print Speed 30ppm or above.
TR 10.213	It shall have Resolution Min 600 x 600 dpi or better.
TR 10.214	It shall have Memory 1 GB or higher.
TR 10.215	It shall have Copy speed 12ppm or better.
TR 10.216	It shall have scanner of Flat Bed type with ADF.
TR 10.217	It shall have Interface USB 2.0, Ethernet Port.

TR 10.218	It shall have the duty cycle of monthly 5000 pages at minimum.
TR 10.219	Full toner Cartridge shall be supplied with the printer.
TR 10.220	It shall have input tray capacity of minimum 100 sheets.
TR 10.221	It shall have output tray capacity of minimum 100 sheets.
TR 10.222	Printer shall be accompanied with the necessary accessories such as connecting cables, driver media, etc.
EPABX System	
TR 10.223	It shall have provision for at least 25 IP Phone extensions. Expandable to 50 Extensions. As part of this solution, 6 EPABX handsets shall be required.
TR 10.224	It shall have 6 Party Internal/External Multi group Tele-conferencing facility to all the Call Takers, Dispatchers and Supervisors/ Managers etc.
TR 10.225	It shall support all the standard features like Call Transfer, Call Forward, Call pick-up, Call hold, Call Barge-in etc.
TR 10.226	At minimum, it shall have 1 Trunk Card of 8 lines with CLI to connect Land Line / GSM Phones.
TR 10.227	It shall have ISDN PRI Cards 4 Nos. at minimum that shall be expandable for 8 Nos.
TR 10.228	It shall have PCM-TDM, IP, Non-blocking as technology.
TR 10.229	It shall support all Telecom interfaces.
TR 10.230	It shall have ISDN interface for digital & Basic interface for Analog lines.
TR 10.231	It shall support analog and IP/ Soft phone.
TR 10.232	It shall have Integrated Voice messaging system with required channels for IVRS function.
TR 10.233	It shall have Voice messaging-Pre-defined text to voice conversion information.
TR 10.234	It shall have an estimated wait time in case if all operators are busy.
TR 10.235	It shall have voice mail instructions to caller in case all the operators are busy.
TR 10.236	It shall have 6 party In and Out Multi group conferencing facility to be provided to all the Call Takers, Supervisor and Manager etc. (To be configurable Dynamically).
TR 10.237	It shall have Digital Extension telephone instrument with programmable one touch keys, Graphical display, Keys with LED, 4 Programmable keys with dual function,10 fixed function keys.
TR 10.238	It shall provide industry tested, proved and market leading switches to ensure smooth installation and protecting businesses existing call centre hardware investment.
TR 10.239	It shall support SIP based communications.
USB KVM Extender	
TR 10.240	The extender shall extend USB, keyboard, audio, video and mouse signals through a single cable CATx cable.
TR 10.241	The extender shall provide control on both the local and remote location. Controls include and not limited to video, keyboard, mouse and USB.
TR 10.242	The extender shall extend signals to a minimum distance of 300m via CATx cable.
TR 10.243	The extender shall automatically synchronizes the time delay of RGB signals to compensate for distance and support Auto Signal Compensation (ASC).
TR 10.244	The extender shall support high resolution video up to 1920 x 1200Hz (150 m); 1280 x 1024 at 300 m.

TR 10.245	The AC input power shall be 110-240 VAC +/- 10% at 50/60 Hz +/- 1Hz.
TR 10.246	The extender shall support auto-negotiable 10/100/1000 Ethernet network.
TR 10.247	The extender shall be operational in temperature between ten degrees Celsius (10°C) to forty degrees Celsius (40°C).
Communication Cabinets with Racks	
TR 10.248	Please refer to the Communications Cabinet with Racks specifications as mentioned under IT Infrastructure Section 2.2.7.3
Local On-Site Servers	
TR 10.249	Please refer to the Servers specifications as mentioned under IT infrastructure Section.2.2.7.4
Other Specification	
Lighting	
TR 10.250	All overhead lighting shall be LEDs both recessed direct and indirect lighting, including pot-lights.
TR 10.251	The overhead lighting treatment shall be incorporated into the other ceiling elements to create an aesthetic specialty ceiling design, in combination with the Rooms.
TR 10.252	Overhead lighting intensity shall be: • For Operations Room: at least 400 lux • For Rack Room: at least 500 lux
TR 10.253	Dimming control shall be continuous (all lights dimmable) and zone-based (with a minimum of 4 lighting zones on separate circuits).
TR 10.254	Dimming control shall have various configurations preset for the ideal operations lighting environment, based on the perimeter glass wall natural lighting conditions (e.g., sunny, cloudy, partly cloudy, night, etc.).
TR 10.255	Appropriate wall boxes for corresponding dimmer size shall be provided. Dimmers shall not be ganged in one box.
TR 10.256	Manual switches shall be used for on / off lighting control and for overriding any preset lighting configurations.
TR 10.257	Cover plates for switches shall match the colour of switches, receptacles, and receptacle cover plates. Cover plates shall be of the same manufacturer as the devices.
TR 10.258	All lighting fixtures shall be of high-grade quality over and above the standard level of quality for office lighting.
TR 10.259	Lighting arrangement shall accommodate console locations.
TR 10.260	Lighting shall be configured in order to reduce glares and reflections on console monitors and on the video wall, as well as accommodate any other lighting needs the monitors and video wall may have.
Ceiling	
TR 10.261	The specialty ceiling treatment shall incorporate the following as a minimum: • Overhead lighting • Suspended audio system components (e.g., speakers) • Fire / CO alarms • Wet sprinklers; and • Sound absorption ceiling tiles
TR 10.262	In the Operations Room, the specialty ceiling treatment shall also accommodate a fill-in wall partition between the upper edge of the video display wall and the ceiling.

TR 10.263	In Rack Room, the ceiling shall be open (to the concrete slab) to allow access to cable and fibre infrastructure and HVAC system. The ceiling slab shall be reinforced to support the fully loaded weight of cable trays, fibre trays, and the overhead electrical (power) raceway. Each of these will be securely fastened to the ceiling slab with either uni-strut bars or hangers and threaded rods.
Floors	
TR 10.264	Flooring with proper acoustic treatment shall be used to reduce the impact sound by at least 14dB.
TR 10.265	A 12 in / 0.30 m raised floating floor shall be installed, bolted to the under structure (i.e., pedestals).
TR 10.266	The raised floating floor shall have the ability to be accessed from any location within the Operations Room and Cabin / Boardroom.
TR 10.267	The baseboard treatment shall extend to conceal the 12 in / 0.3 m raised floating floor.
TR 10.268	The raised floating floor shall be capable of supporting general loading of 600 – 1200 kg / m^3 (123 – 245 lb / ft^2).
TR 10.269	The raised floating floor shall be capable of supporting in excess of the concentrated static loading of the consoles, video wall and loaded equipment racks.
TR 10.270	The raised floating floor shall be grounded.
TR 10.271	The pedestal / supporting structure for the video wall shall be fastened to the concrete slab floor.
TR 10.272	Stub conduits shall be installed in the concrete slab floor (underneath the raised floating floor) of the Operations Room.
Environmental Conditions to be Maintained inside MCC	
Temperature	
TR 10.273	The temperature level shall be set at 23°C +/- 1°C.
Humidity	
TR 10.274	Relative humidity level shall be constant and set to 45% - 55%.
Ventilation	
TR 10.275	The base building specifications i.e. PoP shall cover general pressure requirements.
TR 10.276	The normal pressure shall be maintained.
Acoustics	
TR 10.277	A high level of noise will be generated by MCC activities, therefore sound insulation and sound absorptive measures shall be installed in the Operations Room & Cabin / Boardroom (e.g., ceiling panels / tiles, wall panels).
TR 10.278	In order to mitigate acoustic issues, floor to slab construction is required for all walls and partitions.

3 Detailed Scope of Work

3.1 MSI Scope of Services - Overview

The Project requires turnkey services wherein the MSI shall broadly cover the following main scope of services:

- Design;
- Supply;
- Install;
- Test;
- Integrate;
- Commission; and,
- Operations and maintenance.

The subsequent sections detail out the scope with respect to execution of this Project. The MSI shall note that the activities defined within scope of work mentioned 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 bid document and factor the same in its response.

The following Exhibit 12 presents the detailed scope of services that have to be carried out as a part of the contract.

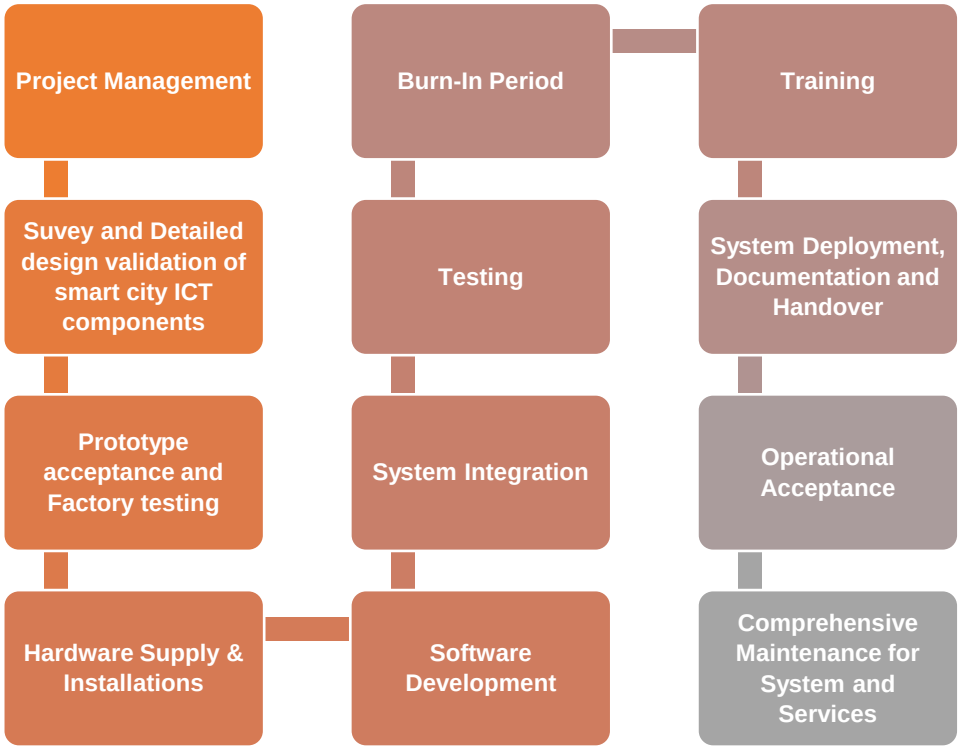


Exhibit 12: Detailed Scope of Work

3.1.1 Project Management

MSI shall be responsible for end to end project management for the implementation and maintenance of the smart city ICT components. MSI shall deploy a competent team of experts for project management which shall include a Project Manager along with a deputy.

The Project Manager shall be the single point of contact that shall assume overall responsibility of the Project and ensure end to end working of the Project. He shall function as the primary channel of communication for all Client requirements to the implementation team. In case of any absence of the project manager (sickness

or vacation), the MSI shall ensure that an alternate project manager (as approved by the client or its representative) shall be provided during the absence period.

As per the finalized staff deployment plan, MSI shall be obligated to ensure availability of Key Experts at the Project location (Mumbai / Aurangabad) during the entire Contract duration. Mechanisms to transparently record and monitor Key Expert availability at project location shall be under the scope of MSI. The MSI shall provide monthly report to the Client providing compliance for availability of Key Expert at Project location.

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

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

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

All the tools required by MSI for project management, configuration management, issue and risk management, escalation procedure and matrix document repository etc. shall be factored in the proposal submitted by MSI. As part of the Project, MSI shall use Primavera P6 as the project management tool. MSI shall submit periodic baseline schedules in Work Breakdown Structure (WBS).

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

All deliverables shall be submitted in at least two (2) formats i.e. draft and final. The Client's representative will have at least 30 days to review and comment on every deliverable. The practice of submissions for all deliverables will be that three (3) hard copies and CDs of every deliverable shall be submitted. Two of these copies will be submitted to the ICT consultant and one will be submitted to the client. The submissions will include both hard and soft copies.

3.1.2 Survey and Detailed Design Validation of all Smart City ICT Components

MSI shall conduct end-to-end survey of the site area, additional requirement gathering and based on the observations, asses and validate the present conditions, implementation approach and methodology, project challenges and mitigations and other project critical information. During the survey stage itself, MSI shall mobilize its entire staff and fully acquaint them with the site conditions. It is MSI's responsibility to periodically survey the site and be updated on the conditions during the course of the contract. During the design validation stage, MSI is also expected to:

- Workshops with different stakeholders for capturing business requirements, creating awareness of best practices, communicating the changes, building consensus on process design etc. These needs to be organized at different intervals and in different places throughout the duration of the projects as needed.
- Stake holder consultation other than workshops, with those stake holders who will be identified by AITL, for critical inputs, review, suggestions, process description etc.
- Review sessions with different stake holders for signing off the deliverables, walking through the deliverables for facilitating quick understanding.

The MSI shall also be responsible for the detailed design validation of the project. MSI shall discuss in detail and validate with the Client or its representatives the detailed design of the smart city ICT components and

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

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

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

- All system device locations as required for installation, operation and maintenance;
- Cable requirements, routing and location (as applicable);
- Typical mounting details;
- Single Line Diagrams (SLDs);
- Splicing diagrams;
- Wiring diagrams;
- 3D layouts and renderings for PoP and MCC;
- Any other layouts;
- Any other requirement to meet the requirements of the RFQ cum RFP.

All drawings shall be updated/revised to "as-built" conditions when installation is complete.

Design submissions shall be based on project requirements and shall include as applicable, but not limited to, the following:

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

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

For the software components, MSI will create requirement analysis documents. This includes System Requirements Specifications (SRS) and the Functional Requirements Specifications (FRS). The MSI shall be responsible for documenting any existing/planned 'processes' of the Client as part of these deliverables. Document shall also clearly illustrate the integration points with existing systems such as AEE modules, Smart City Platform, Building Management System, Video Management System etc. The required customizations and development on these modules shall also be included in detail as part of project report.

As part of the Project, the ICT Consultant shall provide drawings to the MSI in raw format. These drawings include typical details, proposed equipment location, routing and typical splicing. It will be MSI's responsibility to work on these drawings as a base, update them as per the latest site conditions, and convert these drawings to 'for-construction' drawings.

3.1.3 Prototype Acceptance and Factory Acceptance Testing

After the approvals of the technical data sheets by the Client or its representative, MSI shall submit the prototype of the material presented in the Detailed Design Report to the Client or its representative for its review and approval. Note that it shall be MSI's responsibility to get the prototypes approved in due course of time without affecting the overall schedule of completion of works.

Material provided as part of the Project shall undergo Prototype Acceptance Test (PAT) and Factory Acceptance Test (FAT). Details regarding the PAT and FAT are presented in Testing Section of the Scope of

Work. MSI shall also present to the Client and its representatives the test results for PAT and FAT in the form of Test Result Documentation presented in the Testing section. The Client and its representative at their own discretion shall visit any FAT site. MSI shall be responsible for organizing all logistics required for any such site visit.

For all the software components, the MSI shall also propose prototype of solution components as part of this phase and get the required approvals.

3.1.4 Hardware Supply and Installation Stage

MSI shall be responsible for the supply and installation of all components as part of AURIC-Bidkin Phase-1 smart city ICT components to meet the technical, functional, business and performance requirements of this RFQ cum RFP. No deviations from these requirements shall be acceptable by the Client. Any additional hardware or software component required to meet the technical and performance requirement of the project and not specified as part of this document but required to meet the overall requirements of the project shall be factored in as part of the Bid, and provided by the MSI. MSI shall deliver the project and install and handle the equipment in accordance with manufacturer's requirements. Installation process of the MSI shall be flexible and shall accommodate Client's requirements without affecting the schedule as specified in the RFQ cum RFP.

MSI shall be responsible to provide ICT enabled electrical meters for measuring electricity consumption of the Smart City ICT components at Four (4) different places. MSI shall be responsible for all supply, storage and handling of the material provided as part of the project. The OEM proposed for the IT infrastructure shall be in line with the national security policy (as applicable).

If there is removal/change of any existing material during installation process and belongs to the Client, the material shall be handed-over to the Client. MSI shall also be responsible for reinstating any site in the project limits at no additional cost to the client. It shall be the MSI's responsibility to supply and install all hardware in compliance with the requirements of the RFQ cum RFP. Since this is a turnkey contract, MSI shall be responsible for all implementation works on the project including any civil, structural, electrical, etc. works required to meet the requirements of the project. All power conversions necessary to operate the equipment shall be under the scope of MSI. The Client shall only provide raw power for all the equipment.

3.1.5 Software Development

MSI shall be responsible for development and deployment of all software required to meet the requirements of the project. Some of the software may be COTS or may require bespoke development. MSI shall be fully responsible for developing, implementing and integrating all software required for the project.

All software development/ implementation may be demonstrated to the Client periodically in Mumbai as per the project requirements. All software shall be developed based on the approved software and functional requirements specifications. The technology platform chosen for all software shall be based on industry standards based and shall be secure. Migration of data shall be the responsibility of the MSI. MSI is required to take the source data in the format which is available. Subsequently, MSI is required to take complete ownership of data migration and also develop a detailed plan for data migration against the same.

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

MSI shall be responsible for development and customizations which are required for Bidkin specific applications to be integrated with Shendra applications. For example, MSI shall develop and customize the functionalities and interfaces associated with Smart City Platform specific to Bidkin applications.

3.1.6 System Integration

MSI shall be responsible for the integration of all hardware and software supplied as part of this Project as per the technical and performance requirements of the project. The system integration scope also includes integration of the Project components with the components provided by others as per the details of the RFQ cum RFP.

It shall be MSI's responsibility to integrate the software components being developed as part of AURIC-Bidkin Phase-1 with the existing system of AURIC-Shendra. This includes integration of selected software components with the Smart City Platform already operational for AURIC-Shendra, and which shall also be the primary platform for monitoring the smart city ICT elements implemented for AURIC-Bidkin Phase-1. Similarly, MSI shall also undertake integrations associated with AEE, Building Management Systems, Video Management Systems etc. It shall be the responsibility of MSI to take approval of the Client for the Integration of the overall system as per the RFQ cum RFP. Post systems integration, the Client shall review and approve the overall performance of the integrated system as per the requirements of the RFQ cum RFP. MSI shall be responsible for fixing any requirements that are not found in compliance with the original RFQ cum RFP and approved detailed design at no additional cost to the client.

3.1.7 Testing

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

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

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

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

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

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

All measuring instruments required to measure test parameters shall be calibrated by an approved testing authority. The equipment shall be inspected for standards of construction and electrical and mechanical safety.

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

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

ATP shall incorporate the following distinct stages for each deployed stage as mentioned below:

Hardware Component Acceptance Testing Procedures (ATPs):

- **Prototype Acceptance Tests (PAT)**: Prototype Approval Test shall be conducted only on the customised equipment for their design and compliance to functional specifications. PAT shall be completed before conducting FAT and only after approval of PAT by Client's representative, the equipment shall go in production. PAT shall be witnessed by Client's representatives.
- **Factory Acceptance Tests (FAT):** FAT shall be conducted before the equipment is shipped to Client for installation, and deficiencies shall be rectified before shipping to Client for installation. All devices furnished by the MSI shall be tested and subjected to a nominal 72-hours burn-in period at the factory. FAT shall be witnessed by Client's representatives at their discretion.

  Factory acceptance tests shall be conducted on randomly selected final assemblies of all equipment to be supplied. Sample size for FAT shall be a minimum of 10%. In case any of the selected samples fail, the failed sampled is rejected and additional 20% samples shall be selected randomly and tested. In case any sample from the additional 20% also fails the entire batch may be rejected.
- **Pre-Installation Testing (PIT):** All equipment supplied under this Contract shall undergo pre-installation testing in accordance with the ATP. This shall include existing equipment, any spare parts, any new equipment provided by Client or their designate and new equipment provided by the MSI.

  If the equipment is considered a standard production item, the MSI may, with the prior consent of the Client or their representative, supply a copy of the equipment manufacturer's quality control test results in place of a MSI performed test.

  All PIT testing shall be carried out prior to installation of the equipment. After satisfactory completion of the MSI's PIT tests, the MSI shall supply all test measurements and results to the Client or their representative, together with a Test Certificate.
- **Installation Acceptance Tests (IAT):** IAT shall be conducted after each installation of each equipment type, and deficiencies shall be rectified before the initiation of SAT. IAT may be witnessed by Client's representatives.
- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all subsystems installed under this Contract. Where connections of the new systems to existing subsystems or equipment supplied by others are required, the MSI is responsible for connection of equipment specified in the Contract and for initial system integration tests. Such a test will verify the full functionality of each subsystem as they are interconnected. This will require testing to be coordinated by the MSI with the Client or their designate. This work will be carried out under the direction of the Client or their designate.

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

  The MSI shall:

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

A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system.

- **System Acceptance Tests (SAT):** SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of the final Burn-in Period. SAT shall be conducted on full system completion only to determine if the system business, functional and technical requirements as specified in the bidding documents are met. SAT shall be witnessed by Client's representatives. Data migration, if any, will be carried out by MSI prior to commencement of this stage. Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc. shall also be done as part of SAT. Post successful completion of SAT, 'Operation Acceptance Certificate' for the System or the Subsystem which was tested will be issued by the Client. On issuance of Operational Acceptance Certificate for the individual system, the Comprehensive Maintenance phase (AMC Phase) will commence for the system component. Comprehensive Maintenance period for each respective system will continue till for the entire Contract duration, irrespective of the time of successful SAT.

Software Component Acceptance Testing Procedures (ATPs):

- **Software Factory Acceptance Test (SFAT):** In case of all the COTS software components, SFAT will be conducted for that software component at the Software Laboratory before it is delivered to Client for necessary project specific customizations. In case of any customized software, the MSI shall also propose prototype of solution components as part of this test and get the required approvals.
- **System Integration Testing (SIT):** The MSI is responsible for the proper and harmonious operation of all software subsystems developed, installed and integrated under this Contract. This will require testing to be coordinated by the MSI with the Client or their designate. This work will be carried out under the direction of the Client or their designate.

  The MSI shall:

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

  A SIT certificate will be issued when all system tests have been completed satisfactorily, and the MSI has supplied a full set of Test Certificates and a Test Certificate for the complete system.
- **Stress and Load Testing:** Comprehensive stress and load testing of software modules shall be conducted to demonstrate robustness and reliability of the system will be undertaken for approximately 30% of projected population, subject to applicability.
- **Security Testing (including penetration and vulnerability test):** Security test shall be conducted to demonstrate security requirements at network layer and software applications. The software components shall pass vulnerability and penetration testing for rollout of each phase. Components shall also pass web application security testing for in the case of applicable web applications. Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live. Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase. For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.
- **System Acceptance Tests (SAT):** SAT shall be conducted after the entire system has been installed, integrated and commissioned. Deficiencies, if any shall be rectified before the initiation of the final Burn-in Period. SAT shall be conducted on full system completion only to determine if the system business, functional and technical requirements as specified in the bidding documents are met. SAT shall be witnessed by Client's representatives. Data migration, if any, will be carried out by MSI prior to commencement of this stage. Scrutiny of all inspection reports, audit findings, Contracts, licensing agreements etc. shall also be done as part of SAT. Post successful completion of SAT, 'Operation

Acceptance Certificate' for the System or the Subsystem which was tested will be issued by the Client. On issuance of Operational Acceptance Certificate for the individual system, the Comprehensive Maintenance phase (AMC Phase) will commence for the system component. Comprehensive Maintenance period for each respective system will continue till for the entire Contract duration, irrespective of the time of successful SAT.

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

Third Party Testing:

MSI shall get at least 1% of the material to be supplied as part of the RFQ cum RFP tested by a government laboratory such as NABL, TEC (or any other approved by the Client). Third party labs shall test the equipment for their conformance to the RFQ cum RFP requirements. No material shall be supplied on-site without successful third party testing from a government lab. The components that shall undergo third party lab testing shall be decided by the Client or its representative in consultation with the MSI.

Third Party Inspection

MSI shall also be responsible for ensuring third party inspection of all the material supplied as part of the Project from a Government Agency. The tentative scope of work of the third party agency shall be as per following:

- **On Supply of Material:** Third party government agency shall perform an inspection once the material is supplied on-site and before commencement of any installation. Third party government agency shall certify that the material supplied on-site are as per the make & model and quantity approved by the Client or its representative. In addition, it shall also certify that material supplied on-site are in a proper condition and without any damage or wear and tear. In case there is a payment milestone based on supply of material, third party government agency shall also certify the submission of invoices are as per the material supplied on-site.
- **Before System Acceptance Test (SAT):** MSI shall get the system certified by the third party inspection agency before commencing SAT with the Client or its representative. Third party agency shall ensure that business, functional and technical specifications mentioned as part of the RFQ cum RFP are fulfilled by the MSI before calling for official SAT.

All the commercials associated with appointing a third party government agency for inspection shall be included by the MSI as part of the financial proposal. MSI shall submit the names of at least three third party government agencies as part of the Detailed Project Report (DPR) along with their company profile and inspection experience. Client shall approve one third party government agency in consultation with the MSI.

The MSI shall provide written notice to Client at least five (5) days in advance of any testing, indicating the specific tests to be completed as well as the date, time and location. The MSI shall be required to reschedule testing if Client witnessing representatives cannot be present or if other circumstances prevent testing from taking place.

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

<table>
<tr><td colspan="2">Item #:
Item Description:
Test:</td><td colspan="2">Tester:
Date:</td></tr>
<tr><td colspan="4">Test Set-up:</td></tr>
<tr><td>Clause</td><td>Test Procedure</td><td>Expected Results</td><td>Actual Results</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="4">Witnessed:
(This Does Not Constitute Approval)
Reviewed and Approved:</td></tr>
</table>

MSI shall be responsible to carry out all the testing as per the satisfaction of the Client and its representatives. It is the responsibility of the MSI for all documentation required for establishing approval and acceptance of installation and operation of the system components. All the costs those are associated with any testing are to be borne by the MSI including the costs of travel and accommodation of the Client or its representatives from their home locations in their cost bid. In the interest of the MSI maximum of three (3) people shall be nominated by the Client to attend any such testing wherever it is carried out.

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

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

3.1.8 Burn-In Period

Following successful completion of the SAT for all the project components and before final deployment, the approved Systems will be put into service and its performance monitored for a period of thirty (30) consecutive calendar days for the purpose of verifying system reliability in an operating environment. Any failures and defects occurring in this time will be documented. Any serious defects which affect the availability of the system will be a basis for restarting the test. MSI shall also review health, usage and performance of the system till it is stabilized during Burn-in Period. Based on Client's feedback for incorporating changes as required and appropriate, MSI shall train staff involved in the Burn-in Period. Upon the satisfactory completion of this burn in period, a Completion Certificate will be issued.

The MSI shall not commence Burn-in Period until SAT for all the project components have been performed and successfully completed/approved and all documentation of the successful completion of PAT, FAT, PIT, IAT, SIT and SIT, along with notification of the schedule date of the Burn-in Period is provided to the Client or their representative in accordance with the Requirements. Commencement of Burn-in Period will be conditional on the Client or their designate providing written notification of Client's readiness to proceed to Burn-in Period.

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

The Burn-In Period shall be demonstrated to the Client's representatives. If for any reason the burn-in is found to be incomplete or non-compliant, these will be communicated to the MSI in writing on the lapses that need to be made good. A one-time extension will be provided to the MSI for making good on the lapses pointed out before offering the system to Client for review. Failure to successfully demonstrate the burn-in period may lead to termination of the contract with no liability to Client.

3.1.9 Training

Post the system integration, MSI shall train Client and any representatives to operate the implemented systems and to conduct any routine diagnostics and routine maintenance work. Training shall be done during Burn-In Period and before Final Deployment. The period of training shall be mutually agreed upon by Client and MSI.

The MSI shall provide training courses for at least:

- Decision Makers/ Management;
- Client's operations personnel;
- Users of Various Systems/Applications developed as part of the project.

The actual number of each of above categories of trainees will be provided during the course of the Contract.

MSI shall provide all training materials in both Microsoft Office and Adobe PDF formats, consisting of graphics, video and animations on Compact Disc (CD) and Digital Video Disc (DVD) with a permission to reproduce copies later on.

MSI shall also be responsible for full capacity building of AITL staff. Training and capacity building shall be provided for all individual modules along with their respective integrations. All training materials shall be developed by the MSI.

The Training Plan (TP), including the training schedule and course outlines, must be provided to Client for review at least three (3) weeks in advance of the start of training. The TP must be approved by Client before the start of training.

MSI shall furnish all special tools, training videos, self-learning tools, equipment, training aids, and any other materials required to train course participants, for use during training courses. Training shall include, as a minimum, a four (4) hour session on system maintenance and configuration, and a four (4) hour session on system operation.

The instructors shall demonstrate a thorough knowledge of the material covered in the courses, familiarity with the training materials used in the courses, and the ability to effectively lead the staff in a classroom setting. If at any stage of training, the Client feels that on-field sessions are required, the same shall be conducted by the MSI. The language of training shall be in English/Hindi as indicated by the Client during this stage.

If any instructor is considered unsuitable by Client, either before or during the training, the MSI shall provide a suitable replacement within one (1) week of receiving such notice from Client.

The MSI shall provide brief refresher versions of each training course to the original trainees and new inductees between three to six months after System Acceptance for each deployment stage at no additional cost.

MSI shall train 50 staff of the Client during the initial stage. Subsequently, MSI shall train around 25 staff every 3 to 6 months during the contract period.

MSI has to ensure that training sessions are effective and the attendees shall be able to carry on with their work efficiently. For this purpose, it is necessary that effectiveness of the training session is measured through a comprehensive online feedback mechanism.

3.1.10 Final Deployment and Documentation

After addressing the Client feedback and any deficiency observed during completion of data migration, System Acceptance Tests (SAT) and upon Burn-In Period final deployment of the project components shall be considered by the MSI. For achievement of final deployment, MSI shall also be responsible for development of a cutover strategy which shall include initial data take on, sequence of data take on, set up of support mechanisms to minimize business impact due to any cutover activities.

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

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

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

‘As-built’ Documents delivered by the MSI shall include:

- An inventory of all components supplied including model name, model number, serial number and installation location;
- An inventory of all spare parts supplied including brand, model number, and serial number and storage location;
- All reference and user manuals for system components, including those components supplied by third parties;
- All warranties documentation, including that for components supplied by third parties;

- As-builts in CAD and GIS;
- A diagram indicating the as-built inter-connections between components;
- Software documentation which also includes the version number of all software, including that supplied by third parties;
- Cable run lists and schedules;
- All network and equipment details such as IP addresses, user names, and passwords;
- Manufacturer's test procedures and quality assurance procedures for information.
- Data communication protocols; and
- 'As-Built' drawings for all components installed.

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

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

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

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

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

- Business process guides;
- Program flow descriptions;
- Data model descriptions;
- Sample reports;
- Screen formats;
- Frequently Asked Questions (FAQ) guides;
- User Manuals and technical manuals;
- Any other documentation required for usage of implemented solution.

Documentation of processes shall be done using standard flow charting software. An intuitive online learning tool depicting standard operating procedures of system usage are required to be deployed. There shall be a provision of training system in the deployment architecture so as new employees can be inducted easily.

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

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

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

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

3.1.11 Operational Acceptance of the Project

At the successful completion of SATs of all the Project systems and the Burn-In Period, the Project shall be considered for operational acceptance. At the close of the work and before issue of final certificate of completion by the Client, the MSI shall furnish a written guarantee indemnifying Client against defective materials and workmanship for a period of one (1) year after completion which is referred to as Defect Liability Period. The MSI shall hold himself fully responsible for reinstallation or replace free of cost to Client during the Defect Liability period. MSI shall provide approved temporary replacement equipment and material such that the system remains fully functional as designed and commissioned during repair or replacement activities at no cost to the Client.

3.1.12 Comprehensive Maintenance for System and Services

MSI shall be responsible for comprehensive maintenance of both hardware and software, up-gradations in the system, expansion of the system, technical manpower, spares management and replenishment, performance monitoring and enhancements, preventive and corrective maintenance of the AURIC-Bidkin Phase-1 smart city ICT components deployed as part of this project and shall maintain service levels as defined in the RFQ cum RFP. All equipment and material supplied by the MSI shall be provided with standard warranty against defects of design and manufacturing and against faults and failures associated with workmanship of MSI and its sub-contractors commencing from operation acceptance of the system. All equipment found to be defective during comprehensive maintenance shall be repaired or replaced by the MSI at no cost to the Client. Comprehensive Maintenance Phase shall include Defect Liability Period (Warranty Period) and Post-Warranty Service Period.

MSI shall provide all the technical, managerial, and other staffing required to manage day-to-day maintenance of the Bidkin Phase-1 smart city ICT components during the Contract period.

All spares required for the smooth operation of the AURIC-Bidkin Phase-1 smart city ICT components shall be maintained by the MSI for the entire duration of the contract to meet SLA requirements. The cost of the spares, repairs, and replacement shall all be deemed to be included in the price quoted by the MSI. MSI shall also institutionalize structures, processes and reports for management of SLA. Root cause analysis and long term problem solutions shall also be part of MSI scope.

MSI shall maintain all data regarding entitlement for any upgrade, enhancement, refreshes, replacement, bug fixing and maintenance for all project components during Warranty. MSI shall be responsible for updates/upgrades and implementation of new versions for software and operating systems when released by the respective OEM at no extra cost to the Client during entire duration of contract. Requisite adjustments / changes in the configuration for implementing different versions of system solution and/or its components shall also be done by MSI. The MSI shall also ensure application of patches to the licensed software covering the appropriate system component software, operating system, databases and other applications. Software License management and control services shall also be conducted by the MSI during this phase. Any

changes/upgrades to the software during comprehensive maintenance shall be subjected to comprehensive and integrated testing by MSI to ensure that changes implemented in system meets the specified requirements and doesn't impact any other function of the system. Issue log for errors and bugs identified in the solution and any change done in solution (vis-à-vis the FRS, BRS and SRS signed off) shall be periodically submitted to the Client. MSI shall also be responsible for operating all software components of the project including all support, content updates, system updates and upgrades throughout the duration of contract. All the software developments, customizations and integrations, done specific for Bidkin specific applications with the AURIC-Shendra applications such as AEE, smart city platform, VMS etc. shall also be maintained by the MSI.

MSI shall ensure OEM support during Comprehensive Maintenance stage for system performance, performance tuning, calibrations, upgrades etc. MSI shall provide all support for formulation of all policies and procedures related to System Administration, Data Base Management, applications, archives, network management & security, back up and data recovery and archive, data synchronization after crash. Assistance to Client shall be provided as needed in management of legacy data interfaced, print spools, batch jobs, printer configuration etc.

MSI shall prepare a detailed System administration manual, Data administration manual, operational manual, User manual which shall be used by Client's employees to operate AURIC-Bidkin Phase-1 smart city ICT components. This shall also include how the various parameters shall be monitored/ tuned in a live system. Preparation of requisite system configuration for disaster recovery management and fail over system plan shall also be under the supervision of MSI. The MSI shall also maintain the following minimum documents with respect to ICT components:

- High level design of system;
- Module level design of system;
- Integration with AURIC-Shendra's existing services;
- System Requirement Specifications (SRS);
- Any other explanatory notes about system;
- Traceability matrix;
- Compilation environment.

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

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

The communication costs (Internet charges, telephone charges, 3G/4G/GPRS connectivity charges) and any other incidental charges related to maintenance period shall be in the scope of the MSI and considered to be included in the proposal submitted by the MSI for the entire contract duration.

Any planned and emergency changes to any component during maintenance period shall be through a change management process. For any change, MSI shall ensure:

- Detailed impact analysis;
- Change plan with roll back plan;
- Appropriate communication on change required has taken place;
- Approvals on change;
- Schedules have been adjusted to minimum impact on production environment;

- All associated documentation are updated post stabilization of the change;
- Version control maintained for software.

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

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

Comprehensive maintenance of individual systems and services shall commence upon successful completion of System Acceptance Test (SAT) and issuance of 'Operational Acceptance Certificate' by the Client. It should be noted that during the course of the implementation period, SAT of various systems, solutions and services shall happen before the Burn-In Period and Operational Acceptance of the Project. Post successful completion of SATs during implementation phase, respective component shall commence their comprehensive maintenance phase. The comprehensive maintenance of all such respective systems and services shall continue till the completion of the contract period, irrespective of the time comprehensive maintenance phase commenced for these particular systems or services. Applicable SLAs and penalties shall be levied on the systems and services which went into maintenance phase during the implementation period. The applicable penalties for the systems and services shall be deducted during release of the performance security post completion of the implementation phase.

Support Personnel Required

Well trained, efficient and effective support personnel (Engineers) shall be provided by the MSI during the maintenance phase of the project. Any fault originating for the AURIC-Bidkin Phase-1 smart city ICT components shall be addressed by the MSI support staff in the least time possible. The support staff shall work in a shift based system and provide full support coverage and maintain the system as per the SLAs defined. Following Support Personnel shall be deputed by the MSI during the comprehensive maintenance phase:

- MCC Support Engineer
- Two (2) Fibre Optic Support Engineer;
- Integration Support Engineer;
- Four (4) MCC Operators;

Above mentioned Engineers shall be well qualified and trained to support the Client's operational and technical staff in day-to-day operations of the AURIC-Bidkin Phase-1 smart city ICT components provided by the MSI. The staff assigned shall be well qualified to attend to the emergency situations and shall be able to communicate in an effective and efficient manner. Support staff shall be well trained on the smart city ICT components to understand and take necessary action in any kind of situation. Please note above mentioned support personnel shall be available 24X7 at site. MSI shall depute four (4) qualified personnel at MCC as the city operators and shall be involved in day to day management of AURIC-Bidkin and MCC.

In addition to the training to the operations staff during acceptance stage, the MSI shall conduct half-yearly training refreshment sessions to train the new staff inducted by the Client and to enhance the knowledge of the Client's staff operating the AURIC-Bidkin Phase-1 smart city ICT components by adopting "train the trainer" approach.

3.2 System Specific Scope of Services

3.2.1 Fibre Optic Infrastructure

- MSI shall undertake a detailed and comprehensive network architecture design validation of smart ICT components covering all the locations in AURIC-Bidkin Phase-1, IT and physical infrastructure in line with the overall objective and requirements of the project. MSI shall identify the space required for setting up the network infrastructure at each of the location;
- MSI shall be required to undertake the GIS based survey to design the OFC route planning and network topology and share the same with the Client. MSI can make use of the publicly available data and tools such as Google Maps, ArcGIS, and NIC developed maps etc. However, the ownership of the accuracy and validation of the data map information shall be with the MSI;
- The network architecture validation exercise shall involve:
  - Detailed Network architecture covering all locations;
  - Detailed Fibre layout;
  - Detailed Network solution and deployment architecture covering the central infrastructure at MCC, PoP and Cloud.
  - Solution required for managing / monitoring the complete Network Backbone, Distribution and Access Layers.
  - Detailed information security architecture to ensure data privacy as well as security.
  - MSI shall validate Network architecture that includes all of the above along with other design elements like data standards, technology standards, interoperability standards, security architecture and other such guidelines / standards. This shall be prepared in active consultation with Client or its representative;
- MSI shall validate the space requirements for all active electronics with the Client;
- MSI shall factor inclusion of various AITL and Govt. offices and their location, bandwidth requirements, security, LAN/WAN protocols, network topology for each of the Smart City ICT component during design validation;
- The Network Architecture once approved shall be base lined either in part or in whole and the Client shall institutionalize the processes for Architecture Change management to undertake any change in the respective location, as required during the contract phase;
- Designing IP Address Schema:
  - The MSI shall design suitable IP Schema for the entire Network Backbone including MCC, PoP, smart city ICT components and interfaces to external systems/ network. The MSI shall ensure efficient traffic routing irrespective of link medium;
  - The MSI shall maintain the IP Schema with required modifications from time to time within the scope of the project.
- MSI shall coordinate and validate with the Client the detailed cable routing along with locations of joints, terminations etc.;
- EPC Contractor shall provide end-to-end concrete encased trench with dedicated tray for fibre for the backbone fibre optic infrastructure for all RoWs except for 18m or less RoW. MSI to leverage this concrete encased trench and provide any core cutting for implementing its fibre optic infrastructure;
- For 18m or lesser RoW, EPC contractor shall partially provide the HDPE ducts for fibre optic infrastructure with manholes (excluding mounting accessories) at one side of the road. MSI shall use the same ducts for backbone & distribution OFC networking. MSI to approve the procedure and methodology of trenching with Client or its representative prior to any work on site. EPC Contractor shall also provide pipes for any crossings that will be used by the MSI for installation of the fibre optic infrastructure;

- MSI to provide trench for connectivity to plots and devices from the backbone and distribution trench as per the requirements of this RFQ cum RFP. MSI shall coordinate with EPC Contractor for access to streetlight poles for infrastructure connectivity.
- MSI to coordinate with EPC Contractor for all civil requirements and ensure all design requirements are met on-site;
- MSI to assess and incorporate in the implementation the type of soil, long cuttings, new embankments, water logged areas, types of major bridges, major yards etc.;
- MSI to work out the requirements of heavy tools and plants depending upon nature of the territory, availability of roads alongside etc.;
- MSI to work out requirement of transport vehicles like jeeps, lorries, motor trolleys, etc. as needed for execution of the work;
- MSI to provide all manholes with core cutting near to the RMU locations for connectivity to plots and field devices across backbone and distribution network. MSI to coordinate with EPC Contractor for the manhole and handhole/pits locations, detailed design and access. MSI to provide handholes/pits within AITL plots and any additional required for field level connectivity;
- Before carrying out laying and installation of ducts and fibre, MSI shall prepare an installation report (approved by the Client or its representative) which shall constitute the following:
  - Closely examining the proposed cable route and prepared cable route plans;
  - Installation and preparation of site plans for buildings required for the execution of the work, as offices at different stations, store godowns;
  - Siting of areas for loading/unloading of cable drums and siding facilities for the for the project;
  - Preparation of the material schedule required for different protective works;
  - Arranging isolated components circuits to be provided in the cable;
  - Investigation of special problems, if any, of the section and finding out proposed solution thereof.
- MSI is expected to put in practices for precaution against damage by Termites & Rodents;
- Cable laying is proposed either by traditional Cable pulling method or by Cable blowing method (preferably);
- After the cable is laid and splicing is complete, measurements in the below proforma shall have to be prepared and maintained:

Section		**Distance**	**Cable Length**	**Fibre No.**	**Loss in DB**		**Remarks**
From	To				1310 nm	1550 nm	

- MSI shall coordinate with the EPC Contractor for ICT interface for utilities including but not limited to water, power and street lighting infrastructure;
- MSI shall coordinate with TSPs, cellular and any other tenants for their fibre optic infrastructure requirements and any other network requirements. The tenants will be responsible for providing their respective FOSCs and splicing (installation). MSI shall be responsible for supervising this splicing works and any integration;
- MSI shall only be responsible for splicing of backbone, distribution and access network for AITL plots and AITL field devices only;
- For non-AITL plots, MSI shall provide the access duct from the manhole until just outside the property line, where it will be stubbed out for access in the future. Using this duct, the plot developer shall be responsible to provide the dedicated fibre optic infrastructure inside the plot and install the required

fibre optic cable with the FOSC and splicing. In this case, the MSI shall be responsible for full supervision of these works and assistance in integrating this infrastructure end-to-end. For all AITL plots, the MSI shall be responsible for end-to-end fibre optic infrastructure;

- All coordination with plot developers for splicing and integration with AITL fibre shall be under the scope of the MSI;
- MSI shall compute and implement all the storage infrastructure required as part of the fibre optic infrastructure. All networking and firewall requirements for the fibre optic infrastructure will also need to be undertaken by MSI;
- MSI shall be responsible for data encryption and data security;
- Provide details on connection type, speed and bandwidth required at the MCC and PoP (as applicable) for connectivity to outside world;
- Maintain the fibre asset management system during the course of the contract;
- Proper earthing, grounding and lighting suppression for all applicable equipment under the scope of MSI.
- MSI shall be responsible for supply and installation of all manholes/handholes/pits, wherever required.

3.2.1.1 PoP Rooms

- MSI shall be required to undertake the complete site preparation, plot development including plot boundary in compliance with the DC regulations and design-build exercise for three (3) PoP facilities as per the requirement in consultation with Client and its representative;
- The detailed design in all aspects for the design-build (including but not limited to civil, mechanical, structural, electrical, communications, fire, fit-outs, etc.) of the PoP facility and the plot shall be the responsibility of the MSI and be approved by the Client or its representative. The MSI shall have the required personnel on the team including architect, structural engineer, MEP, etc. as needed for this design-build. At least two (2) options for the design-build shall be proposed for the PoP facility;
- This scope includes finalization of locations of the PoP, development of the building, development of the plot in compliance with the regulations including necessary infrastructure within the plot, fencing, coordination with the tenants, coordination for installation of cellular towers and any other infrastructure of the tenants, partitioning for dedicated space for every tenant, and construction of the PoP facility;
- All tenants will get dedicated partitioned space for their equipment along with access to power and other basic infrastructure. MSI shall ensure that the passive infrastructure in terms of ducts, termination points, etc. for routing within the PoP is provided for all tenants. MSI shall coordinate with all tenants to ensure end-to-end installation of all the tenant provided equipment. All tenant space shall have dedicated access, be secure and should be modular in construction so that the number of tenants can be increased or decreased in the future;
- MSI shall furnish the PoP rooms as part of the civil work in all aspects. All material to be used shall be of fine quality ISI marked or equivalent. The furnishing includes but not limited to:
  - Trench works;
  - Masonry works;
  - Cutting and chipping of any existing area;
  - Glazing;
  - False ceilings;
  - False floorings;
  - Paint work;
  - Storage;

- Layouts and partitioning;
- Doors and Locks;
- Fire detection;
- Cement concrete works;
- Insulation.

- MSI shall install electrical distribution system in the buildings. MSI shall be responsible for proper and uninterrupted equipment working and shall ensure this by having the telecom equipment and server room power distribution with redundancy:
  - Incoming electrical feeder supply;
  - UPS system with battery bank for all AITL loads;
  - Connection between UPS system and the AITL equipment shall be redundant. No single point of failure shall exist in the power connectivity between the AITL equipment and UPS.
- Since PoP room is a critical area, precise air conditioning system shall be exclusively installed by MSI to maintain the required temperature for the AITL area only. All AC units shall be redundant such that failure of one does not impact the operating temperature required to be maintained in the AITL area;
- MSI shall install UPS system to provide redundant power supply to following needs:
  - All AITL equipment;
  - Access control;
  - Fire detection and gas suppression system of PoP facility as per the specifications.
- MSI shall do complete electrical cabling work for telecommunication equipment which shall include but not limited to:
  - Main electrical panel in room;
  - Power cabling;
  - UPS distribution board;
  - UPS point wiring;
  - Power cabling for utility points and utility components etc.;
  - Online UPS;
  - Separate earth pits for the component;
  - MSI shall use fire retardant cables of rated capacity exceeding the power requirements of equipment to be used at maximum capacity;
  - All material shall conform to ISI standards as per industry practice.
- MSI shall be responsible for the lighting works in the building. Following items need to be undertaken by MSI for lighting:
  - Supply of all equipment associated with implementation of lighting including fixtures, lamps, wiring etc.;
  - Wiring for lighting system in the building;
  - Installation of lighting fixtures;
  - Warranty for the lighting equipment;
  - Critical lights shall be connected to UPS for uninterrupted lighting;
  - Post the installation, MSI shall ensure that lux levels of the building are as per IES-HB-10-11.

- The facility shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards;
- The Access card based access control system shall be deployed by the MSI with the objective of allowing entry and exit to and from the premises to only authorized personnel with appropriate door locks and controller assembly. It shall be installed at entry and exit of PoP rooms and MCC. In addition, it shall also be installed at AITL partition area inside PoP. Access Control system shall be IP enabled and integrated with the BMS. Access control system shall also be enabled with attendance management system for AITL staff. The attendance management system shall be integrated with AEE SAP-ERP by the MSI. All equipment associated with implementation of Access Control including wiring, workstation etc. shall be under MSI scope.
- A web enabled Building Management System (BMS) shall be implemented by the MSI at PoPs including the MCC area. BMS shall enable building managers to monitor, control and automate various systems in the building via an integrated platform from a central location. All accessories associated with the BMS including central application, Workstation, Direct Digital Controllers (DDCs), cabling, conduiting, sensors etc. shall be under the scope of MSI. MSI shall integrate following systems with the BMS for centralized monitoring:
  - Air Conditioning System;
  - Lighting System;
  - DG parameters (if applicable);
  - Energy consumption of the building through metering;
  - Video Surveillance of PoP premises;
  - Access Control System;
  - UPS;
  - Fire Alarm and Fire Suppression System;

  MSI shall also develop an I/O summary with exhaustive integration capabilities and submit it to the Client for review. Since, BMS is a design-build exercise, MSI shall ensure compatibility of all PoP systems such as Air Conditioning, Lighting, UPS etc. with BMS. The MSI shall integrate BMS parameters with the Smart City Platform at AURIC-Shendra. All works associated with integration of Bidkin BMS with Smart City Platform including any associated development or customizations at Smart City Platform shall be under the scope of the MSI
- MSI shall also be responsible for installing a rodent repellent provision inside the PoP facilities.
- Required land for PoP will be provided by Client. Location for PoP shall be shared with successful Bidder.

3.2.2 Public Wi-Fi

- The MSI shall validate through a coverage modelling and/or detailed survey in AURIC-Bidkin (Phase-1) area the number of hotspots required;
- The MSI shall have a Wi-Fi operator, Licensed ISP in India who shall be able to meet all requirements for operations of network as per RFQ cum RFP who will be responsible for operating this Wi-Fi network. The Wi-Fi network operator shall be a neutral operator i.e. a tenant based model where any licensed service provider may offer Wi-Fi services using this network;
- The MSI shall be responsible for monetization of City Wi-Fi services in compliance with the requirements of the RFQ cum RFP;

- The APs shall be installed at street light poles and kiosks. MSI shall coordinate closely with EPC Contractor responsible for providing these street light poles;
- Raw bandwidth required for the city Wi-Fi network shall be provided at no additional cost by the MSI. Internet bandwidth from ISP to Wi-Fi shall be under MSI scope;
- Testing of Wi-Fi network for penetration, security and coverage post deployment of the network;
- The MSI shall comply with all the standards and best practices. MSI shall also ensure that DoT and TRAI guidelines issued from time to time including but not limited to security, user registration, equipment EIRP, etc. At no point Client or its authorized entities shall be responsible for any non-compliance on account of non-adherence by the MSI;
- The MSI shall develop and implement a billing and accounting software for e-recharge, enabling Wi-Fi usage and accounting for the service revenue as per the requirements stated in this RFQ cum RFP;
- MSI shall also be responsible for:
  - Providing Technical manpower, for the contract period from the date of acceptance, to look after the day to day management of services related to Wi-Fi facility management. These services shall include:
    - Providing connectivity to user devices as per requirements of this RFQ cum RFP and in consultation with the Client or its representative;
    - Satisfactorily handling all the issues related to connectivity, performance and security.
  - Providing adequate security mechanisms in City Wi-Fi service equipment to prevent unauthorized access or interfaces to services, calls, protocols and data;
  - The MSI shall provide all the usage data/log/analysis for further usage like usage prediction, planning towards additional resource deployment

3.2.3 City Surveillance with ATCC and ANPR Cameras

- MSI shall install CCTV Cameras at all strategic locations including roads, intersections, public spaces/buildings, and other critical/sensitive facilities like Mini Control Centre and PoP Rooms;
- MSI shall be responsible for integrating the City Surveillance System with the City Infrastructure;
- MSI shall be responsible for establishing the mechanisms;
- MSI shall be responsible for setting up required infrastructure for exchange of video feeds and alarms/ notifications between the Mini Control Centre (at AURIC-Bidkin Phase-1) and the AURIC Control Centre (at AURIC-Shendra);
- MSI shall be responsible to optimize the network architecture design and to calculate the overall bandwidth requirements to transmit the Video feeds of AURIC-Bidkin Phase-1 to ACC as per the finalized agreement with the Client.
- MSI shall be responsible for any additional compute (servers) and storage required for AURIC – Bidkin Phase-1 City Surveillance video data at AURIC Control Centre in Shendra. MSI shall coordinate with Shendra MSI if there is a requirement of additional storage and servers at ACC in order to integrate the Bidkin's City Surveillance System;
- MSI shall be responsible to provide local server and storage equipment a minimum at MCC for storing the video feeds;
- MSI shall conduct a survey and prepare a detailed report on the basis of which locations, positions, mounting arrangements and height, orientation/field of view of the CCTV cameras shall be finalized;
- MSI shall be responsible for making proper adjustments to have the best possible image/video captured. MSI to also ensure cameras are protected from on-field challenges of weather, physical damage and theft;

- MSI shall be responsible for integrating all the CCTVs being installed at AURIC-Bidkin's Phase-1 area with the Honeywell's Digital Video Manager (DVM) R600 located at AURIC Control Centre (ACC) at Shendra. Any additional licenses as part of this deployment shall be provided by the Bidkin-MSI.
- MSI shall be responsible for integrating each CCTV with the central application server by providing the unique ID, IP addresses, etc.
- MSI shall be responsible for data encryption and data security of the videos recorded;
- MSI shall coordinate with the EPC Contractor for installation of CCTVs on streetlights.

3.2.4 Multi-Services Digital Kiosks and Emergency Communications

- MSI shall be responsible for creating the required software platform to support the functionalities of the Multi-Services Digital Kiosk;
- MSI shall be responsible for integrating the VoIP features at the ACC for transferring the call to the respective departments;
- MSI shall be responsible for integrating the each kiosk with the central application server by providing the unique ID, IP addresses, etc.;
- MSI shall be responsible for upgrading the OS, firmware and other related platform of the Kiosk periodically;
- MSI shall be responsible for replenishment of consumables including paper for printing receipts and tickets;
- MSI shall be responsible for carrying out the turnkey works for implementing the kiosks;
- MSI shall coordinate with the EPC Contractor and other plot developers for installation and Right of Way (RoW).
- 10 Wi-Fi hotspots as part of Kiosk are additional to the requirement of 75 access points asked in the BoQ.
- Kiosks shall be installed outdoors, although a few of the kiosks might be installed indoors. Locations to be finalized by MSI with the Client and its representative.

3.2.5 Environmental Sensor

- MSI shall be responsible for integration of the proposed environmental sensors at Bidkin Phase-1 with the existing PAQS environmental sensor application operational in Shendra. MSI shall be responsible for all the necessary coordination for integration with AURIC-Shendra MSI. Any customizations, development, licensing implication etc. involved with integration of additional environmental sensors with PAQS application shall be under the scope of MSI.
- MSI shall be responsible for integration of environmental sensor data with the smart city platform at ACC. Any development, customizations, interface curation required for integration of environmental sensor with ACC smart city platform shall be under the scope of MSI.
- MSI shall implement a Digital Display Screen (DDS) to display environmental parameters to the public. MSI shall be responsible for all civil, electrical and communication works to implement DDS. The DDS shall also be integrated with the Smart City Platform at ACC.

3.2.6 ICT Interface for Water, Power and Streetlight Infrastructure

- EPC Contractor shall provide SCADA based water, power and streetlighting infrastructure, integrated at the respective reservoirs and substations. Preliminary information on this infrastructure is as follows:
  - All water, power, streetlight, wastewater infrastructure shall be SCADA enabled.
  - Each plot shall have a dedicated water and power meter (both AMR based) respectively;
  - Existing streetlight control system (SCADA) is from Crompton make.

- EPC Contractor will develop a Central Control Room (CCR) where all the SCADA feeds will be integrated and monitored;
- Finalized architecture of the SCADA systems shall be provided to the MSI during design phase. MSI is expected to work in close coordination with the EPC contractor and ensure all integrations as per the finalized design requirements are catered to.

- Coordinate with EPC Contractor to successfully integrate this infrastructure at the ACC. MSI shall take all the SCADA feed from the CCR to be integrated with ACC. It is expected that not all functionality of this infrastructure will be duplicated at the ACC but only critical parameters shall be enabled at the ACC. This shall be finalized by the MSI in consultation with the Client, the EPC Contractor and the ICT consultant;
- EPC Contractor shall provide water and power meters with in-built M2M communications module. MSI shall work with the EPC Contractor to finalize the communications requirements of these meters and integrate them with the overall system;
- Integrate the operations and maintenance of this infrastructure with the AURIC e-Governance and ERP (AEE);
- MSI in consultation with EPC Contractor shall implement Streetlight Gateways including all associated accessories. Integration of Streetlight Gateways with the central Crompton application shall also be under MSI scope. Any licenses required to integrate gateways with the Crompton's existing central management software shall also be the responsibility of the MSI.

3.2.7 Chatbot Solution for Investor Management

- The MSI shall be responsible for end-to-end development, installation, customization, integration, operations and maintenance of all the software and hardware components related to the implementation of Chatbot solution for investor and citizen query(ies) and grievance management.
- The MSI shall work closely with the Client to customize the operations of Chatbot over the entire duration of the Contract including Comprehensive Maintenance Phase.
- MSI shall be responsible for seamless integration of Chatbot with ACC's Smart City Platform, e-Governance services and SAP-ERP. All integration requirements, development, customizations associated with smart city platform, e-Governance application and SAP-ERP in regards to Chatbot solution shall be under the scope of MSI.
- Chatbot solution is also intended to be a marketing tool for AURIC. All content development and curation in case of Chatbot solution including development of FAQs, reply to customer queries, automatic email generations etc. shall be under the scope of MSI.
- Cloud migration and backup of the Chatbot solution shall be under the scope of MSI.

3.2.8 AURIC-Bidkin Mini Control Centre (MCC)

- The detailed design in all aspects for the design-build (including but not limited to civil, mechanical, structural, electrical, communications, fire, fit-outs, furniture, etc.) of the MCC shall be the responsibility of the MSI and be approved by the Client or its representative. The MSI shall have the required personnel on the team including architect, structural engineer, MEP (Mechanical, Electrical and Plumbing), etc. as needed for this design-build. At least two (2) options for the design-build shall be proposed for the MCC;
- MCC shall be housed in the Primary PoP. Area of MCC shall be approximately 1000 Sq. Ft. MCC area shall consist of MCC operations room including operator consoles with video wall, a cabin/boardroom for management and decision making, a sitting gallery and a rack room for equipment. Implementation of MCC operations room, boardroom, sitting gallery and rack room shall be done by MSI;
- MSI shall take consultation and approval of Client or its representative, for the interior layout and material to be procured for MCC;

- MSI shall furnish the MCC as part of the civil work in all aspects. All material to be used shall be of fine quality ISI marked or equivalent. The furnishing includes but not limited to:
  - Trench works;
  - Masonry works;
  - Cutting and chipping of any existing area;
  - Glazing;
  - False ceilings;
  - False floorings;
  - Paint work;
  - Storage;
  - Layouts and partitioning;
  - Doors and Locks;
  - Fire proofing of all surfaces;
  - Cement concrete works;
  - Insulation.
- MSI shall install electrical distribution system inside the MCC. MSI shall be responsible for proper and uninterrupted equipment working and shall ensure this by having the IT equipment and server room power distribution with redundancy:
  - Incoming HT/LT feeder supply;
  - UPS system with battery bank for all AITL loads.
  - Connection between UPS system and the IT equipment shall be redundant. No single point of failure shall exist in the power connectivity between the IT equipment and UPS.
- Since MCC is a critical area, dedicated redundant air conditioning system shall be exclusively installed by MSI to maintain the required temperature. The A/C shall be capable of providing sensible cooling capacities at ambient temperature and humidity with adequate air flow. The task of MSI shall include but not limited to:
  - Connecting the indoor unit with main electrical point;
  - Connecting indoor and outdoor units mechanically (with insulated copper piping);
  - Connecting indoor and outdoor unit to power;
  - The air conditioning shall be linked to a secondary power supply as redundant source to prevent them from shutting down in case of power outage;
  - Air conditioning shall be redundant with no failure.
- MSI shall do complete electrical cabling work for IT equipment which shall include but not limited to:
  - Main electrical panel in room;
  - Power cabling;
  - UPS distribution board;
  - UPS point wiring;
  - Power cabling for utility points and utility components etc.;
  - Online UPS;
  - Separate earth pits for the component;
  - MSI shall use fire retardant cables of rated capacity exceeding the power requirements of equipment to be used at maximum capacity;
  - All material shall conform to ISI standards as per industry practice.

- MSI shall be responsible for the lighting works in the facility. Following items need to be undertaken by MSI for lighting:
  - Supply of all equipment associated with implementation of lighting including fixtures, lamps, wiring etc.;
  - Wiring for lighting system in the building;
  - Installation of lighting fixtures;
  - Warranty for the lighting equipment;
  - Critical lights shall be connected to UPS for uninterrupted lighting;
  - Post the installation, MSI shall ensure that lux levels of the building are as per IES-HB-10-11 and requirements of this RFQ cum RFP.
- The MCC shall be equipped with adequate and advanced Fire Detection and Suppression system. The system shall raise an alarm in the event of smoke detection. The system shall have proper signage, response indicators and hooters in case of an emergency. The system shall be based as per NFPA standards;
- The Access card based access control system shall be deployed by the MSI with the objective of allowing entry and exit to and from the premises to only authorized personnel with appropriate door locks and controller assembly. It shall be installed at entry and exit of MCC. Access Control system shall be IP enabled and integrated with the BMS. Access control system shall also be enabled with attendance management system for AITL staff. The attendance management system shall be integrated with AEE SAP-ERP by the MSI. All equipment associated with implementation of Access Control including wiring, workstation, software including programming of the software etc. shall be under MSI scope.
- MSI shall also install CCTV surveillance system inside MCC for video surveillance of the facility. The MSI shall also provide the MCC operations room to be Wi-Fi enabled;
- MSI shall also be responsible for installing a rodent repellent provision inside the MCC facility;
- MSI shall be responsible for compliance with all local standards and certifications, including building, electrical and occupational requirements;
- MSI shall aggregate and integrate all Bidkin specific application at MCC. MSI shall coordinate with relevant stakeholders for integration of any external or third party system;
- MSI shall integrate MCC and all its associated applications with Cisco CKC (smart city platform) at AURIC Control Centre (ACC) in Shendra. All Bidkin specific developments, customizations, interface creation and integrations at the Cisco CKC platform shall be under the scope of MSI;
- All analytics associated with AURIC-Shendra systems is done via SAS Analytics platform. All Bidkin specific development, customizations, interface creation and integrations at the SAS Analytics Platform shall be under the scope of MSI.
- Connectivity requirements for integration between MCC and ACC shall be under the scope of MSI. The MSI shall provide adequate bandwidth that all applications at MCC including video are integrated at ACC;
- MSI shall also enable a parallel feed of Smart City Platform (Cisco CKC and SAS Analytics) at MCC from ACC for viewing, monitoring and control purposes. Control of only Bidkin specific applications shall be enabled with the parallel feed;
- MSI shall coordinate with Shendra MSI i.e. HAIL, Cisco and SAS for integration of MCC with ACC;
- Any additional compute (servers), storage or any other requirement associated with integration of Bidkin applications with Smart City Platform at ACC or scaling up of applications due to additional requirements shall be under the scope of MSI.

- MSI shall deploy four (4) City Operators at MCC full time who shall be responsible for operations of AURIC-Bidkin and MCC. All manpower related requirements for MCC operators shall be under the scope of MSI.
- Define SOPs with the Client or its representative for the operations to ensure that MCC systems are configured to support the operational procedures;
- Creation of KPIs and dashboards as per the requirement of the Client;
- Build and certify MCC as per ISO 27001:2011 and ISO 11064 standards.

3.2.9 Hosting (On-Premises and Cloud)

- For hosting of all applications, an overall hybrid architecture of on-site infrastructure and infrastructure provided by the cloud service provider shall be considered;
- All servers provided by the MSI shall be in clustered configuration and shall be highly available. The server infrastructure provided by AITL through the cloud service provider shall be of high availability (typically 99.95%). MSI shall ensure that all applications are designed to support the high availability requirement of the infrastructure;
- All application level redundancy, scalability, reliability, etc. requirements shall be under the scope of the MSI;
- As part of the Bid, Bidders shall define the expected storage, server requirements for all stages of the contract for the applications that will be hosted on-cloud;
- Hosting environment shall be in compliance with the Cloud Security Alliance (CSA) Cyber Security Guidelines for Smart City Technology Adoption;
- During the design and implementation stage of the project, the MSI shall provide a cloud architect as part of the team;
- MSI shall recommend system architecture for all the applications for both on-premises and cloud hosting;
- MSI shall provide Disaster recovery, back-up solution, specify/confirm RTO (Recovery time objective), RPO (Recovery point objective), Clustering/high-availability, Single sign on, proposed application uptime, proposed Application response time for all applications, and their respective storage requirements over the implementation and O & M period;
- MSI shall only be responsible for the application level performance and uptime and not that of the availability of the hardware infrastructure being provided by the cloud service provider. However, the MSI shall be fully responsible to work hand-in-hand with the cloud service provider and ensure that an overall highly available solution is provided for the project;
- All applications deployed on cloud shall support required cloud architecture and shall be auto-scalable.
- MSI shall only get Infrastructure as a Service from AITL's cloud service provider. All installation/operations, management and operations of the MSI provided services and applications shall be performed by MSI. The Cloud Service Provider shall not provide managed services for installation but will only provide infrastructure that can be accessed and managed by the MSI. The MSI shall be responsible to ensure the optimized functioning of the infrastructure at any given time during the course of the Contract. MSI shall provide managed services for operations and maintenance of the cloud infrastructure for all applications;
- MSI shall be responsible for complete support and maintenance during phase-wise commissioning as well;
- Cloud Service Provider for AURIC is ESDS Software Solutions Pvt. Ltd. MSI shall coordinate with ESDS in consultation with the Client or its representative for hosting of applications on cloud. MSI shall be responsible for optimizing cloud compute and storage required for its respective application.

- As part of the Project, below mentioned MSI applications shall be hosted on cloud. All other applications implemented for this project shall be hosted on-premises by the MSI.
  - Chatbot Solution for Investor Management;
  - DDS software.

3.2.10 Integration with AURIC e-Governance and ERP (AEE)

As a part of the AURIC e-Governance and ERP (AEE), multiple applications have been provided for Shendra (or are in a very advanced stage of implementation) for both the citizens and businesses as well as for internal AITL stakeholders. The main system components of the AEE are:

- Customer Facing Systems: Multi-Channel Communication Centre for citizens, Portal, e-governance functions, M-Governance Functions, Social Governance, Web based GIS layer, Digital Locker, Citizen Smart Card, Kiosk and Mobile Applications, Management Information System along with KPI and Dashboards;
- Back office systems i.e. the SAP ERP S/4 Hana comprising of finance & accounts, purchasing, budgeting, contract management system, asset management, water connection, billing, maintenance, project stores HR & payroll
- Framework for integrating various applications like Document Management System (New Gen), Land Management System, Web GIS and any other application.

The vision of AITL is to use IT towards establishment of people centred, responsive, well governed functions and to provide a single, easy, secure and reliable means to deliver municipal information and services to citizens. A citizen facilitation centre, multi services digital kiosks, mobile application and website backed with an integrated portal is the front end of these applications.

AITL recognizes the importance of Information Technology (IT) to enhance the efficiency and effectiveness of service delivery to citizens and stakeholders. Due to this, AITL has set up a vision to develop a fully digital organization by comprehensive deployment of IT across its departments of conduct business. As part of the vision, it has been envisaged to implement electronic delivery of AITL services to citizens for greater efficiency, transparency and accountability.

3.2.10.1 E-Governance

The following modules are implemented for AURIC:

- **e-LMS:** to process applications for land allotment and all related documentation
- **Corporate Website:** to provide useful information to citizen and stakeholders.
- **AITL Portal and Mobile Applications:** a gateway to all stakeholder experience including citizens.
- **Citizen Facilitation Centre (CFC):** in person contact point for all citizens.
- **Birth and Death Certificate Module**: capability for online registration of birth and death certificates.
- **Trade Licenses:** to issue and for periodic review and approval of licenses.
- **Right to Information (RTI):** to provide information to accept applications, register requests, disposal to relevant department, track status, maintain an appeal register and status of appeals.
- **Legal – Related to Land only:** to assist the legal cell of AITL to monitor and analyze all land related cases and expenditures.
- **Citizen Grievance Redressal:** an online module for citizens to register and track all public grievances associated with AITL functions through the AITL portal and mobile application.
- **GIS Platform with Web GIS:** a web enabled version of the GIS map implemented for citizens and AITL employees linked to different modules. WebGIS in particular has been developed for AURIC-Shendra only. For WebGIS development works of AURIC-Bidkin, the Bidkin MSI shall be responsible.
- **Management Information System (KPI Dashboard):** An abstract of all modules together with city indicators.

- **Digital Locker:** an online file storage facility for citizens and businesses.
- **Smart Card System:** a digital identity for investors for easy access and to avail services from AITL.
- **Automated Building Plan Approval System:** an online solution to AITL for building layout plans scrutiny.

All the above mentioned modules are integrated with the back-office systems via middleware SAP Process Orchestration (PO) to function as one cohesive and holistic system which shall play a vital role in electronic and automated service delivery to citizens.

3.2.10.2 SAP, Document Management & E-Auction

The following modules are implemented for AURIC:

- **Revenue Management;**
- **E-Auction for Land;**
- **Finance and Management Accounting:**
  - General Ledger;
  - Accounts Payable and Receivable;
  - Asset Management;
  - Management and Cost Accounting;
  - Capital Investment Planning;
  - Costing.
- **Purchasing and Inventory Management;**
- **Contracts Management;**
- **Operations Maintenance and Asset Life Cycle Management;**
- **Project and Works Management;**
- **HR and Payroll System;**
- **Enterprise Content Management/Document Management System;**
- **Water Utility Management and Billing.**

The AEE system comprises of modules developed for AURIC-Shendra, which have catered to the functionality requirements of AURIC-Bidkin as well. In most cases the integration and implementation effort will be for an extension of the existing systems which would be performed by this MSI. The scope of work of Bidkin MSI shall be as per below:

- The MSI is strongly advised to study the current functionality/scope of the existing AEE systems as a part of their technical bid and the Project. Any gaps observed during this study shall be accounted for as part of the MSI's scope.
- Adhere to the business processes prescribed by the AEE systems and provide the necessary assistance and collaboration for integrating Bidkin Phase-I to AEE.
- Any development and customization required for extending and integrating AEE systems shall be undertaken by the MSI in coordination and support with the Shendra MSI.
- In the case of web GIS, MSI will ensure that the shape files for land parcels, ICT infrastructure for Bidkin and maps created are provided to the Shendra MSI for uploading.
- Provide the Shendra MSI support for AEE systems with the required master and transaction data in the prescribed format, to enable the extension of the AEE system to Bidkin.

- Take initiative and ownership and proactively collaborate with the Shendra MSI, in providing any other support required to extend AEE to Bidkin which includes building interfaces for all relevant systems as determined by AITL. The nature of these interfaces shall be online .For example, these systems include SCADA, Automated Meter Readers, Digital Kiosks, State and Central Govt. portals, Police & Fire brigade and other AITL needs as and when they arise. Any software modifications required for compatibility and/or integration shall be carried out by the MSI as part of this RFQ cum RFP.
- All verification of the migrated data for Bidkin on the AEE system components will be the responsibility of the MSI. Data cleansing ownership would also lie with the MSI.
- MSI shall take full ownership and the onus of integration and productive use of the AEE along the online integration of the specific systems being installed/developed/implemented as a part of this RFQ cum RFP.
- Content development and curation associated with any AEE module integrated or extended for Bidkin application shall be under the scope of MSI. At any given time, one Content Developer shall be available for creation of new content during the entire course of the Contract, Content Developer shall be responsible for content development for AURIC.

3.2.11 Telecom Connectivity between Shendra and Bidkin Phase-1

- MSI shall be responsible for establishing end-to-end telecom connectivity via feasible wired link between AURIC-Bidkin Phase-1 and AURIC-Shendra. The link established by the MSI shall be operational as per the SLA with minimal points of failure and network downtime. In case of any downtime, the MSI shall ensure that there is no packet/data loss and upon restoration the link is live with data transmission starting from the time of point of failure
- MSI shall be responsible for purchasing bandwidth from any of the Telecom Service Provider(s) active in the project area on behalf of AITL along with any associated Active/ Passive infrastructure required for facilitation of telecommunication link between Shendra and Bidkin Phase-1. It shall be MSI's responsibility to ensure appropriate bandwidth availability for transmission of data as per the requirements of the RFQ cum RFP;
- The telecommunication link established by the MSI between AURIC-Bidkin Phase-1 and AURIC-Shendra shall be used to transfer data associated with ICT components of the Project. As part of the project, it is envisaged that data from MCC shall be transmitted to ACC for integration purposes. MSI to ensure all Bidkin specific data is transmitted to ACC.
- All Bidkin specific application data shall also integrate with smart city platform at ACC. Data from applications such Wi-Fi Management System, ATCC system, ANPR system, Environmental Sensors etc. shall be transmitted over the communication link. An additional feed of smart city platform shall also be made available at MCC. MSI shall ensure bandwidth availability for smart city platform feed at MCC.
- The telecommunication link established by the MSI between AURIC-Bidkin Phase-1 and AURIC-Shendra shall be geographically redundant network with minimal points of failure;
- MSI shall be responsible for the overall operations and maintenance of the leased line link including the Active/Passive infrastructure established for exchange of smart city ICT data from AURIC-Bidkin Phase-1 to AURIC –Shendra. MSI shall be responsible for comprehensive maintenance of the communication link between AURIC-Shendra and Bidkin Phase-1 till the completion of the Contract period.

4 Roles and Responsibilities

4.1 Master Systems Integrator (MSI)

MSI shall be responsible for providing a complete system that incorporates all specification requirements, including but not limited to:

- Provide all components as per the project requirements;
- Establish the required connectivity between AURIC-Bidkin Phase-1 and AURIC-Shendra as per the project requirements;
- Provide full assistance and support for facilitating integration(s) for the system(s) newly developed / extended between AURIC-Bidkin Phase-1 and AURIC Control Centre (at AURIC-Shendra);
- Deployment of a competent team of experts for each system solution with relevant prior experience and depth of knowledge in each functional area. Team of experts shall be able to supervise end to end business processes for all project components;
- Scheduling the activities and accordingly deploying the resources in a pragmatic manner in order to complete the implementation of the smart city ICT components within the required scope, quality and time constraints;
- Project Team and Management: Since the continuity of the key members of the project team is essential, MSI to follow diligent process for ensuring continuity of key personnel assigned for implementation of the project. For project team, MSI shall carry out following responsibilities:
  - At the project initiation, the MSI will share the profiles of the “Key Personnel” with Client and these key profiles shall meet the minimum eligibility criteria highlighted in the RFQ cum RFP as well as the proposal submitted by the MSI;
  - Regular meetings between key personnel and the Client or its representative to discuss project implementation and progress;
- Deployment of a project structure for effective governance, monitoring, review and risk mitigation;
- Provision of all testing services, up to and including the System Acceptance Test;
- Provision of all Installation and Configuration services defined as part of bid document;
- Provision of detailed Documentation for the MSI’s solution;
- Provision of all Training and associated documentation for Client’s personnel;
- MSI shall provide Project Quality services as following:
  - Adoption of standard methodology encompassing project documentation at various phases, following robust review mechanisms and ensuring quality at all the stages of the project;
  - The MSI is expected to deploy all the quality assurance mechanisms as per international quality standards for this project;
  - ICT systems shall be deployed in such a manner that they are scalable and upgradations of hardware and software are possible with minimal efforts. MSI shall include product upgrade as part of scope during installation;
  - Detailed quality assurance plan for all the phases of the project shall be provided by the MSI.
- MSI shall be responsible for the following feedback, monitoring and adoption mechanism:
  - Stakeholder Mapping : The MSI will put together a structure and mechanism for ensuring that all the relevant stakeholders are consulted, feedback adopted and key differences identified, so as to facilitate standardization as well as user adoption;

- MSI shall indicate the deliverables which shall go for internal review and accordingly the level of expertise that will be deployed for the reviews and the deliverables which will follow quality assurance plans;
- If any of the deliverables are not accepted by the Client, it shall have the right to seek deployment of experts from MSI to review the deliverables. Client shall also hire third party experts to review the deliverables, if required;
- Mechanism to adopt feedback/audit findings: There are three types of feedback for the deliverables – from the users/stake holders, from the internal experts of the MSI and the third party experts hired by AITL. The following is expected from the MSI on these feedbacks/audit findings:
    - All the feedback shall be discussed with Client and based on the guidance of Client, the feedback shall be incorporated into the project;
    - Since the feedbacks/audit findings for any rework is by nature correcting the inadequacy of quality of the work produced in the first place, Client will not accept any change notice requests for these reworks;
    - MSI shall build in adequate mechanisms to control the risks of time over runs possibly due to effort required to rework bad quality deliverables;
    - MSI shall indicate in the beginning of each phase how it plans to take feedback and the mechanisms to incorporate the feedbacks into the project plan and deliverables;
    - MSI shall report to Client how the feedbacks have been incorporated into the project deliverables and take a sign off from the designated authority of Client.

- Provide warranty for all equipment and software, up to and following System Acceptance, and provision of a system warranty following System Acceptance;
- Provide all spare parts for the MSI solution to meet the SLA requirements;
- Provide technical support services following System Acceptance;
- Third Party Inspection by Government agency and testing of samples in Government accredited labs shall be under MSI scope;
- MSI to coordinate with Client, EPC Contractor and other necessary stakeholders to complete the civil and electrical work as required;
- MSI to coordinate with Shendra MSI for any integration requirements with Shendra application (such as AEE, VMS, Smart City Platform, etc.) and ACC.
- MSI shall be responsible for any development, customizations and integration related to Bidkin systems with Shendra systems such as AEE, VMS, Smart City Platform, etc. Any additional licenses, storage and servers required for integrating Bidkin Systems with Shendra systems shall be under the scope of MSI.
- MSI to coordinate with all necessary stakeholders involved in the project for successful and smooth implementation;
- MSI shall work closely with EPC Contractor to meet the requirements of the Project;
- MSI shall provide all the integration support and develop necessary API, program and necessary development to integrate AURIC-Bidkin operations with MCC and ACC, ERP systems and e-Governance applications;
- Temporary power during construction/implementation stage to be arranged and paid by MSI. Client shall only provide power during operations phase;
- Temporary internet connectivity at site for general use and demonstration purposes shall be under MSI scope.

- Last mile power connectivity including any cabling from DB to respective field device to be provided by MSI;
- MSI shall be responsible for demonstrating software development/implementation to the client periodically in Mumbai as per the project requirements;
- MSI shall be responsible for providing training for relevant personnel;
- MSI shall provide secured storage of all equipment on-site;
- MSI shall be responsible for opening and maintaining of project office in AURIC throughout the course of the Contract. MSI shall also setup and maintain office on-site during implementation period. MSI to ensure that temporary office shall have dedicated space for at least two (2) ICT consultants;
- MSI shall depute an on-site project coordinator in Mumbai during the entire implementation period;
- MSI shall provide maintenance support for system and field equipment;
- Client may at any anytime during the contract period choose to undertake an independent third party audit of the implemented system including both application and infrastructure audit. The MSI shall support this audit;
- All reinstatement works shall be under the scope of the MSI;

4.2 Client

Through its authorized personnel and representatives AITL shall:

- Provide basic infrastructure (i.e. space and access) required at each facility for installation of System equipment and for Training;
- Client shall provide land for the PoP rooms;
- Shall approve any provision of raw electricity up to mains power distribution panel at PoP rooms, other sites and training;
- Client shall pay the electricity bill for the smart city ICT components under the scope of this contract during operations phase;
- Assign a Project Manager with the authority to make decisions (and/or designate representatives with such authority) on behalf of Client;
- Participate in all scheduled project activities, attend scheduled meetings and promptly respond to new meeting requests, requests for information, technical support or other necessary communication activities;
- Provide staff, and facilities for all Training held in accordance with the Training Plan;
- Participate and approve the results of all tests, in accordance with the Test Plan;
- Provide payment gateway for all financial transactions;
- Provide internet connectivity for Bidkin applications to Cloud Service Provider facility;
- Provide SMS gateway for SMS;
- Provide Infrastructure-as-a-Service through Cloud Service Provider;
- Provide assistance and support for all types of integration(s) between the AURIC Control Centre and the newly deployed smart city services for AURIC-Bidkin Phase-1, including the Mini Control Centre (MCC);
- Provide base shape files for GIS works to be undertaken by the MSI;
- RoW within project area to be provided by Client at no cost to the MSI;
- Any coordination or permits required for performing works in the project area;

- Client shall assist the MSI in:
  - Obtaining necessary permits or permissions for any activities requiring outside authorization;
  - Coordinating logistical arrangements to receive project related equipment at project facilities;
  - Providing access to field implementation locations as required;
  - Timely acquisition of required technical data from EPC Contractor or other parties;
  - Obtaining any new, changed, or updated operational information necessary for the MSI to configure and initialize the system; and
  - Scheduling and coordination for staff participating in training sessions as per the agreed training schedule.

5 Implementation Schedule (Activities, Milestones and Deliverables)

MSI shall deliver all project activities/milestones/deliverables to the Client as per the timelines stated in this section. MSI shall submit at least two (2) versions of each deliverable as per following:

- Draft Version;
- Final Version.

Client or its authorized representative shall take thirty (30) days to review and provide comments on all respective deliverables. MSI shall ensure that all comments provided by the Client or its authorized representative shall be incorporated in the final version of all deliverables.

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

ACTIVITIES/ MILESTONES/ DELIVERABLES	EXPECTED DATE OF DELIVERY/ COMPLETION FROM CONTRACT SIGNING (D)
Mobilization of Resources	D + 20 Days
Setup of Project Office	D + 1 Month
Submission of Project Plan and Detailed Project Report including all applicable Datasheets and Shop Drawings	D + 1 Month
All Design and Engineering drawings	D + 45 Days
Testing, Commissioning & Integration Plan for Phase-1	D + 3 Months
Testing for Phase 1	D + 5 Months
System Acceptance + Go-Live of Phase-1	D + 6 Months
Testing, Commissioning & Integration Plan for Phase 2	D + 6 Months
Testing for Phase 2	D + 7 Months
System Acceptance + Go-Live of Phase 2	D + 8 Months
Testing, Commissioning & Integration Plan for Phase 3	D + 8 Months
Testing for Phase 3	D + 9 Months
Testing, Commissioning & Integration Plan for Phase 4	D + 9 Months
System Acceptance + Go-Live of Phase 3	D + 10 Months
Testing for Phase 4	D + 10 Months
System Acceptance + Go-Live of Phase 4	D + 11 Months
Completion of One-month Burn-in period + Handover of all systems (Operational acceptance of the Project)	D + 12 Months
Handover of Final As-Builts, Training manuals, Maintenance manuals, User manuals etc.	D + 14 Months
Completion of Defect Liability Period (DLP) and Commencement of Post-Warranty Service Period	D + 24 Months
Completion of Post- Warranty Service Period	D + 84 Months

Appendix A: Standards (for Reference only)

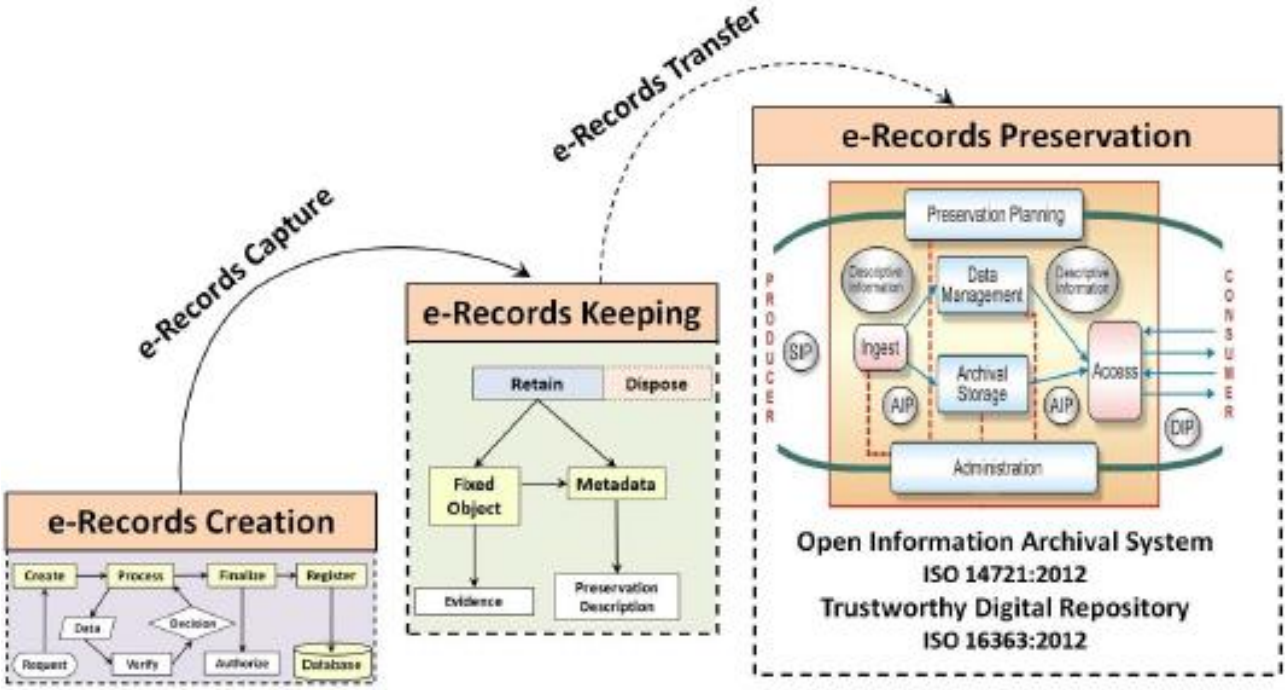
1. Digital Preservation Standards

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) -

STANDARD	DESCRIPTION
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: • PDF/A-1b preserves the visual appearance of the document • Digitized documents in image format can be composited as PDF/A-1b **PDF/A for e-governance applications** • 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** • Libre Office 4.0 supports the exporting of a document in PDF/A format. • MS Office 2007 onwards the support for “save as” PDF/A is available. • 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: • Support for JPEG2000 image compression • Support for transparency effects and layers • Embedding of OpenType fonts • Provisions for digital signatures in accordance with the PDF Advanced Electronic Signatures – PAdES standard • 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.

2. Localization and Language Technology Standard

- **Character Encoding Standard for Indian Languages**

  Standardization is one of the baselines to be followed in localization. Standardization means to follow certain universally accepted standards, so that the developers could interact through the application. Standardization 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.

  Unicode shall be the storage-encoding standard for all constitutionally recognized Indian Languages including English and other global languages as follows:

SPECIFICATION AREA	STANDARD NAME	OWNER	NATURE OF THE STANDARD	NATURE OF RECOMMEND ACTIONS
Character Encoding for Indian Languages	Unicode 5.1.0 and its future upgradation as reported by Unicode Consortium from time to time.	Unicode Consortium, Inc.	Matured	Mandatory

- **Font Standard for Indian Languages**

  A single International Standard to comply with UNICODE data storage. This ensures data portability across various applications and platforms.

  ISO/IEC 14496-OFF (Open Font Format) 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.

  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.**

  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.

3. Metadata and Data Standards

Standardization of data elements is the prerequisite for systematic development of e-Governance applications.

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:

- **Mechanism for allocation of reference no**. to the identified Generic data elements, and their grouping.
- **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
- **Specifications of Code Directories like:**
  - Ownership with rights to update
  - Identification of attributes of the Code directories
  - Standardization of values in the Code directories
- **Metadata of Generic Data Elements:**
  - Identification of Metadata Qualifiers
  - Metadata of the data elements
- **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:

- ISO Standard 1000:1992 for SI Units
- MNIC Coding for Person Identification
- ISO 693-3 for International language codes
- RGI's coding schemes for Languages
- Top level document provided by Working Group on Metadata and Data Standards
- EGIF (e- Government Interoperability Framework) Standard of U.K.
- uidai.gov.in/UID_PDF/Working_Papers/A_UID_Numbering_Scheme.pdf
- http:// www.dolr.nic.in for conversion table of units as used by Department of Land
- Records
- GoI Policy on open standards version 1.0 released in November, 2010
- UID DDSVP Committee report, Version 1.0, Dec 09, 2009
- ANSI92 Standard

4. 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 following are the main measures laid down:

- Web sites of all Government Departments and Agencies shall be made mobile compliant, using the "**One Web"** approach.
- **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.
- **Uniform/ single pre-designated numbers** (long and short codes) shall be used for mobile-based services to ensure convenience.

5. Guidelines for Indian Government Websites

It is suggested that the Indian Government websites adhere to certain common minimum standards, as prerequisites for a Government website to fulfil its primary objective of being a citizen centric source of information & service delivery.

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 (Standardization Testing Quality Certification) an organization 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.

- **Indian Government Entity**

  All websites and Portals belonging to the Indian Government Domain at any hierarchical level (Apex Offices, Constitutional Bodies, Ministries, Departments, Organizations, 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:

  - 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.

  - The Homepage and all important entry pages of the website MUST display the ownership information, either in the header or footer.

  - 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:

    - This Website belongs to Department of Heavy Industries, Ministry of Heavy Industries and Public Enterprises, Government of India' (for a Central Government Department).
    - This Website belongs to Department of Industries, State Government of Maharashtra, India' (for a State Government Department).
    - 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).
    - This is the official Website of the District Administration of Thanjavur, State Government of Tamil Nadu (India)' (for a District of India).

  - All subsequent pages of the website should also display the ownership information in a summarized 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.

  - 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.

- 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.

- **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 .

- **Link with National Portal**

  - **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.

    - **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.**
    - **The pages belonging to the National Portal MUST load into a newly opened browser window of the user.** This will also help visitors find information or service they could not get on that particular website. It is quite common that citizens are not aware which information or service is provided by which Department.

As per linking Policy of the National Portal, no prior permission is required to link 'india.gov.in' from any Indian Government website. However, the Department providing a link to the National Portal is required to inform the National Portal Secretariat about the various sections of the National Portal that they have linked to, so that they can be informed of any changes, updations / additions therein. Also, it is not permitted that the National Portal Pages be loaded into frames on any site. These must be loaded into a new browser window.

Special Banners in different sizes and colour schemes for providing a link to the National Portal have been given at http://india.gov.in/linktous.php

Instructions on how to provide a link have also been given. The Government websites / portals may choose any banner from the ones provided, depending upon their site design and place the same on their Homepage.

- **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.

- **Content Hyper linking**

Since Government websites often receive queries and requests from owners of other websites who might want to provide a hyper link to their web pages, every Indian Government website MUST have a comprehensive and clear-cut hyper linking policy defined and spelt out for those who wish to hyper link content from any of its sections. The basic hyper linking practices and rules should ideally be common across the websites of a State/Ministry.

The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of **'Hyperlinking Policy'** and displayed at a common point on the Homepage of all sites under the ownership a State/Ministry.

- 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.
- 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.

- 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.
- 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.

- **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 endeavor 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.

6. Open APIs

Policy on Open Application Programming Interfaces (APIs)

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.

The objectives of the policy are to:

- Ensure that APIs are published by all Government organisations for all e-Governance applications and systems.
- Enable quick and transparent integration with other e-Governance applications and systems.
- Enable safe and reliable sharing of information and data across various e-Governance applications and systems.
- Promote and expedite innovation through the availability of data from e-Governance applications and systems to the public.
- 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:

- The relevant information being provided by all Government organizations through their respective e-Governance applications shall be open and machine readable.
- All the relevant information and data of a Government organization 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.
- All Open APIs built and data provided, shall adhere to National Cyber Security Policy.
- The Government organizations shall make sure that the Open APIs are stable and scalable.
- All the relevant information, data and functionalities within an e-Governance application or system of a Government organization shall be made available to other e-Governance applications and systems through Open APIs which should be platform and language independent.
- A Government organization consuming the data and information from other e-Governance applications and systems using Open APIs shall undertake information handling, authentication and authorization through a process as defined by the API publishing Organization.
- Each published API of a Government organization shall be provided free of charge whenever possible to other Government organizations and public.
- Each published API shall be properly documented with sample code and sufficient information for developers to make use of the API.
- The life-cycle of the Open API shall be made available by the API publishing Government organization. The API shall be backward compatible with at least two earlier versions.
- All Open API systems built and data provided shall adhere to GoI security policies and guidelines.

- Government organizations may use an authentication mechanism to enable service interoperability and single sign-on.

The policy shall be applicable to all Government organizations 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.

7. Internet of Things

- **Sensor & Actuators**
  - **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.
  - **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.
  - **Domain Specific Compliance:**

    Sensors/IoT Devices/Actuators should follow the compliance to respective domain specific standards, like healthcare devices HL7, OBD-II, Electric Vehicle Charging etc.

- **Communication Technology**
  - **Thread:**

    Networking protocol called Thread that aims to create a standard for communication between connected household devices.
  - **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.
  - **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
  - **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
  - **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
  - **IETF Constrained Application Protocol (CoAP):**

    It offers simplicity and low overhead to enable the interaction and management of embedded devices.

- **Use Case/ Application Specific:**
  - **Industrial IoT (IIoT):** Object Modeling Group (OMG) has been active in IIoT standardization efforts. OMG IIoT standards and activities include (but are not limited to):
    - Data Distribution Service (DDS)
    - Dependability Assurance Framework For Safety-Sensitive Consumer Devices
    - Threat Modeling
    - Structured Assurance Case Metamodel
    - Unified Component Model for Distributed, Real-Time and Embedded Systems
    - Automated Quality Characteristic Measures
    - Interaction Flow Modeling Language™ (IFML™)

    (Source: http://www.omg.org/hot-topics/iot-standards.htm)
  - **eHealth:** IEEE has many standards in the eHealth technology area, from body area networks to 3D modeling of medical data and personal health device communications. IEEE 11073 standards are designed to help healthcare product vendors and integrators create devices and systems for disease management.
  - **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.

- **Consortia**
  - **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.
  - **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.

- **Architecture Technology**
  - **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.

- **Further Readings for Standards**
  - **ITU Standardization Roadmap**

    This document was released on 6 May 2016. It contains a collection of Standards/ITU-T Recommendations that fit into the scope of Joint Coordination Activity for IoT and Smart Cities. It includes Standards/ITU-T Recommendations related to Internet of Things (IoT), smart cities and communities (SC&C), network aspects of identification systems, including RFID (NID) and ubiquitous sensor networks (USN). Refer References for the link.
  - **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.