

# AMRITSAR SMART CITY LIMITED

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



## Detailed Project Report For Implementation & Maintenance of Smart Solutions (Phase - I) in Amritsar City

## Proprietary Notice

This document contains confidential information of ASCL which is provided for the sole purpose of permitting the recipient to evaluate the proposal submitted herewith. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from ASCL or becomes publicly known through no fault of recipient, from ASCL or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to ASCL.

## Disclaimer

This report is intended solely for the information and use of the management of Amritsar Smart City Limited (ASCL), a Special Purpose Vehicle (SPV) Company incorporated under Companies Act, 2013 implementing Smart City Projects in Amritsar City under Smart City Mission of Ministry of Urban Development (MoUD), Govt. of India and is not intended to be and should not be used by anyone other than the specified parties. Project Management Consultant (PMC) therefore assumes no responsibility to any user of the report other than Amritsar Smart City Limited (ASCL). Any other persons who choose to rely on our report may do so entirely at their own risk. Amritsar Smart City Limited act as an implementation agency on behalf of Punjab Municipal Infrastructure Development Company (PMIDC), a State PSU under the Department of Local Government, Punjab for implementation of Smart City projects under Smart City Mission (SCM) in Amritsar City.

### Errors and Omissions

When reading this document if you identify any errors or omissions please advise the author in writing, in 15 calendar days, giving a brief description of the problem, its location within document and your contact details.

### Confidentiality

This document contains privileged and confidential information pertaining to the "Selection of Master System Integrator for Implementation and Maintenance of Smart Solutions (Phase - I) in Amritsar City". The access level for the document is specified above. The addressee should honour access rights by preventing intentional or accidental access outside access scope.

## Glossary of Terms

Abbreviation	Description
AC	Alternate Current
ACL	Access Control List
AMC	Annual Maintenance Contract
ANPR	Automatic Number Plate Recognition
API	Application Program Interface
ARP	Address Resolution Protocol
ASCL	Amritsar Smart City Limited
BOD	Biochemical Oxygen Demand
BOM	Bill of Material
BOQ	Bill of Quantity
BPDU	Bridge Protocol Data Unit
CAD	Computer Aided Dispatch
CCC	Command and Control Centre
CCN	Change Control Note
CEO	Chief Executive Officer
CMOS	Complementary metal-oxide-semiconductor
COC	City Operations Centre
COD	Chemical Oxygen demand
DC	Data Centre
DC	Direct Current
DG	Diesel Generator
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DO	Dissolved Oxygen
dpi	dots per inch
DR	Disaster Recovery
ECB	Emergency Call Box
EMS	Enterprise Management System
ERP	Enterprise Resource Planning
FRS	Functional Requirement Specifications
Gbps	Giga bits per second
GI	Galvanized Iron
GIS	Geographical Information Systems
GoI	Government of India
GPRS	General Packet Radio Services
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GUI	Graphical User Interface
HDD	Hard Disk Drive
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure

Abbreviation	Description
HVAC	Heating, Ventilation and Air conditioning
ICCC	Integrated Control & Command Centre
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IGBT	Insulated-gate Bipolar Transistor
IGMP	Internet Group Management Protocol
IMAP	Internet Message Access Protocol
INR	Indian Rupee
iOS	iPhone Operating System
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6
ISE	Ion Selective Electrodes
ISI	Indian Standards Institute
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Indian Standard Time
ITIL	Information Technology Infrastructure Library
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LCD	Liquid Crystal Display
LDP	Label Distribution Protocol
LED	Light Emitting Diode
LIU	Light Interface Unit
LLDP	Link Layer Discovery Protocol
LOI	Letter of Intent
LPU	Local Processing Unit
MAC	Municipal Corporation Amritsar
MAC	Media Access Control
MCCB	Moulded case Circuit Breaker
MIS	Management Information System
MLD	Multicast Listener Discovery
MoUD	Ministry of Urban Development
MPLS	Multi-Protocol Label Switching
MSI	Master System Integrator
MSTP	Multiple Spanning Tree Protocol
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control

Abbreviation	Description
NAMP	National Air Monitoring Programme
NAS	Network-attached Storage
NAT	Network Address Translation
NEMA	National Electrical Manufacturers Association
NOC	Network Operations Center
NTP	Network Time Protocol
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OFC	Optical Fiber Cable
ONVIF	Open Network Video Interface Forum
P2P	Point to Point
PAS	Public Address System
PDU	Power Distribution Unit
PMIDC	Punjab Municipal Infrastructure Development Company
PoE	Power over Ethernet
PSU	Public Sector Unit
POP	Point of Presence
PTZ	Pan Tilt Zoom
PWM	Pulse-width Modulation
QoS	Quality of Service
RFC	Request For Comment
RoHS	Restriction of Hazardous Substances
RSTP	Rapid Spanning Tree Protocol
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SD-WAN	Software-defined Wide Area Network
SFP	Small form-factor Pluggable
SFTP	Shielded Foiled Twisted Pair
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SOP	Standard Operating Procedure
SPV	Special Purpose Vehicle
SRS	Software Requirements Specification
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
TAN	Total Ammonia Nitrogen
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TRAI	Telecom Regulatory Authority of India
TSS	Total Suspended Solids
UAT	User Acceptance Testing

Abbreviation	Description
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
USD	United States Dollar
VaMS	Variable Message Signboards
VESDA	Very Early Smoke Detection Apparatus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMS	Video Management System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WSDL	Web Service Description Language

## Table of Contents

Proprietary Notice.....	2
Disclaimer .....	2
Glossary of Terms.....	3
Table of Contents .....	7
1. Project Background.....	16
1.1 Smart City Mission .....	16
1.2 Smart Cities in Punjab .....	16
1.3 Project Background.....	18
1.4 Project Implementation Phase .....	20
1.5 Project Stakeholders and their roles.....	21
2. City Surveillance .....	23
2.1 Existing Solutions (As-Is Study).....	23
2.1.1 Amritsar Police .....	23
2.1.2 Existing Surveillance Camera Location Details.....	24
2.1.3 Existing Infrastructure Details.....	29
2.2 ASCL requirement for Security Surveillance .....	30
2.2.1 Requirement for Surveillance for Citizen.....	30
2.2.2 Need of Security Surveillance in Amritsar City.....	31
2.2.3 Amritsar Police intends to implement a city-wide Security Surveillance system with the following objectives.....	31
2.3 Air Quality Analyzer Sensor .....	33
2.3.1 Brief History of Punjab Pollution Control Board .....	33
2.3.2 Details about Punjab Air Laboratory .....	33
2.3.3 List of Ambient Air Quality Stations (NAMP) in the State of Punjab .....	34
2.3.4 List of Ambient Air Quality Stations (NAMP) in the Rural Area of Punjab.....	34
2.3.5 Functions of Punjab Pollution Control Board.....	34
2.3.6 Comparative Values of RSPM, SO <sub>2</sub> & NO <sub>x</sub> µg/m <sup>3</sup> for the years 2013-2017 .....	36
2.4 Online Waste-Water Quality Management System for Drainage Canals in Amritsar City... ..	39
2.4.1 Overview.....	39
2.5 Communication Network .....	41
2.5.1 Geographical Scope .....	41
2.5.2 Existing Network Backbone .....	41
2.6 Integrated Command Control Centre .....	42

2.6.1	IT Enablement of Emergency Systems in Amritsar.....	42
2.6.2	Ambulance – Dial 108.....	42
2.6.3	Fire.....	43
2.6.4	Dial 112 – Project in Amritsar .....	43
3.	Scope of Work .....	44
3.1	General Scope of Work.....	44
3.2	City Surveillance.....	45
3.2.1	Installation of Standard and Cantilever GI Poles.....	46
3.2.2	Outdoor Cabinets / Junction Boxes .....	47
3.2.3	Civil and Electrical Works.....	48
3.2.4	Grounding, Earthing, Bonding and Surge Protection Measures .....	49
3.2.5	IP Camera Surveillance .....	49
3.2.6	Automatic Number Plate Recognition.....	50
3.3	Public Address system.....	51
3.4	Emergency Call Box with Panic Button.....	52
3.5	Air Quality Monitoring Stations .....	52
3.6	Online Waste Water Quality Monitoring System .....	53
3.7	Communication Network .....	54
3.7.1	General Guidelines .....	54
3.7.2	Leasing of Network.....	55
3.7.3	Fault Restoration Services .....	56
3.7.4	Examination of Finished Work .....	58
3.7.5	System Security Safeguards and Risk Mitigation Strategy.....	58
3.7.6	Commissioning of Active / Passive Equipment's and Infrastructure.....	58
3.7.7	Training and Capacity Building.....	59
3.8	Integrated Command Control Centre .....	59
3.8.1	Setting up ICCC (Integrated Command Control Centre).....	60
3.8.1.1	Survey and Site Preparation.....	60
3.8.1.2	Delivery .....	60
3.8.1.3	Installation and Commissioning .....	60
3.8.1.4	Acceptance Testing.....	61
3.8.1.5	Manuals .....	62
3.8.1.6	Product License .....	62
3.8.1.7	Facility Management Services.....	62
3.8.1.8	Electrical System .....	62
3.8.1.9	Diesel Generator .....	63

3.8.1.10	UPS.....	63
3.8.1.11	Cooling Systems or HVAC.....	63
3.8.1.12	Integrated Building Management System .....	64
3.8.1.13	Other Infrastructure Management services .....	64
3.8.1.14	Other Infrastructure or Services.....	65
3.8.1.15	Warranty and AMC .....	65
3.8.1.16	Transportation.....	65
3.8.1.17	Go Live of the project .....	65
3.9	City Operation Centre (COC) for Municipal Functions at ICCC .....	66
3.10	Control and Command Centre (CCC) for Police Functions at ICCC .....	66
3.11	Integration of ICCC with Dial 112 project .....	67
3.12	Data Centre.....	68
3.12.1	Overall DC Architecture .....	68
3.12.2	ASCL Data Centre.....	69
3.12.3	Site Preparation.....	71
3.12.4	Setting up NOC (Network Operations Centre)/ SOC (Security Operations Centre) .....	72
3.12.5	Disaster Recovery and DR Cloud .....	73
3.12.6	Application Design, Development, Procurement, Delivery, Configuration, Implementation, Testing, Commissioning, Operations & Maintenance .....	73
3.12.7	Compliance to SLA.....	80
3.12.8	Application Maintenance.....	80
3.12.9	Problem identification and Resolution.....	81
3.12.10	Application Change & Version Control .....	81
3.12.11	Maintain configuration information.....	81
3.12.12	Maintain configuration information.....	82
3.12.13	Provide Change Control .....	82
3.12.14	Provision, deployment and supervision of manpower for Operations & Maintenance of ASCL Smart Solutions.....	82
3.13	Design and Implementation of Disaster Recovery Infrastructure for ICCC project .....	82
3.13.1	Preparation of Disaster Recovery Operational Plan.....	85
3.13.2	Configure proposed solution for usage .....	85
3.13.3	Periodic Disaster Recovery Plan Update.....	86
4.	Detailed Costing of Integrated Command and Control Centre .....	Error! Bookmark not defined.
4.1	Details Cost (CAPEX + OPEX).....	Error! Bookmark not defined.
4.2	Total Manpower Cost .....	Error! Bookmark not defined.
4.3	Total Overall Estimated Cost .....	Error! Bookmark not defined.

5.	Project Implementation Timelines, Deliverables and Payment Terms .....	87
6.	Service Level Agreement.....	90
6.1	Purpose.....	90
6.2	Service Level Agreement & Targets .....	90
6.3	Measurement & Target .....	91
6.4	Implementation SLA Matrix.....	92
6.5	Operations SLA Matrix .....	94
6.5.1	Data Hosting & IT Infrastructure at ICCC .....	94
6.5.2	Communication Network.....	97
6.5.2.1	Performance levels for leased Network .....	97
6.5.3	Security SLA.....	98
6.5.4	City Surveillance .....	99
6.5.5	Environment Sensor .....	104
6.5.6	Water Quality Analyser.....	105
6.5.7	Fleet Tracking .....	107
7.	Functional Requirement Specifications .....	109
7.1	Field Infrastructure Functional Requirements.....	109
7.2	City Surveillance.....	109
7.2.1	Objectives of strengthening Security Surveillance.....	109
7.2.2	Surveillance System Sub-Components .....	111
7.2.3	General Functional Requirements.....	112
7.2.4	Video Management & Recording System.....	113
7.2.5	Video Analytics.....	121
7.2.5.1	Face Recognition System (FRS) .....	129
7.2.5.2	Automatic Number Plate Recognition (ANPR).....	132
7.2.5.3	Crowd Detection and People Counting in Camera View .....	134
7.2.5.4	Privacy Masking.....	135
7.2.5.5	Un-Attended Objects.....	135
7.2.5.6	Vehicle Count .....	136
7.2.5.7	Vehicle Detection and Tracking Techniques .....	136
7.2.5.8	Wrong way driving .....	137
7.2.5.9	Motion Detection Video Analytic .....	137
7.2.5.10	Perimeter Protection .....	137
7.2.5.11	Congestion Detection .....	138
7.2.5.12	Video Management System (VMS).....	138
7.3	Public Announcement (PA) System.....	143

7.4	Emergency Call Box (ECB) System.....	145
7.5	Air Quality Monitoring System .....	145
7.6	Water Quality Analyser .....	146
7.7	Integrated Command Control Centre .....	148
1.1.1	ICCC Platform Overview.....	148
7.7.1	ICCC Platform Functional Requirements .....	149
7.7.2	Network Operation Centre (NOC) Function Requirement .....	151
7.7.3	Data Centre Functional Requirements .....	154
7.7.4	Cyber Security Framework.....	155
7.7.4.1	Network Behaviour Analysis & Detection.....	157
7.7.4.2	Authentication, Authorization and Accounting (AAA).....	158
7.7.4.3	Internal and Internet Firewalls.....	159
7.7.4.4	Intrusion Prevention system.....	159
7.7.4.5	Web Security Solution .....	159
7.7.4.6	Anti-APT .....	160
7.7.4.7	Web Application Firewall.....	160
7.7.5	Seating Capacity and IT/Non IT Equipment .....	160
7.7.6	Non IT - Civil Infrastructure: Guidelines and Specifications.....	161
7.7.7	Non IT – Electrical Cabling: Guidelines and Specifications .....	181
7.7.8	Non IT – Earthing Network: Guidelines and Specifications .....	187
7.7.9	Non IT – Diesel Generator: Guidelines and Specifications .....	190
7.7.10	Non IT – UPS: Guidelines and Specifications.....	193
7.8	Communication Network .....	201
8.	Technical Specifications Hardware.....	202
8.1	City Surveillance.....	202
8.1.1	Standard GI Pole.....	202
8.1.2	Cantilever GI Pole .....	202
8.1.3	Fixed Box Outdoor Camera - Face recognition, ANPR and General Surveillance .....	203
8.1.4	Bullet Indoor Camera - Face recognition.....	205
8.1.5	360 Degree Panoramic Camera.....	208
8.1.6	PTZ Camera .....	210
8.1.7	Public Address System with Integrated Audio Amplifier.....	211
8.1.8	CAT 6 Cable .....	213
8.1.9	IR illuminator.....	214
8.1.10	Emergency Call Box with Panic Button.....	214
8.1.11	ANPR LPU (Inside Junction Box) .....	215

8.1.12 Body Camera.....	215
8.1.13 Docking System .....	217
8.2 Environment Sensor.....	217
8.2.1 Air Quality Monitoring Station.....	217
8.2.2 Carbon Mono Oxide (CO) Sensor .....	218
8.2.3 Ozone (O <sub>3</sub> ) Sensor.....	218
8.2.4 Nitrogen Dioxide (NO <sub>2</sub> ) Sensor .....	219
8.2.5 Sulphur Dioxide (SO <sub>2</sub> ) Sensor .....	219
8.2.6 Carbon Dioxide (CO <sub>2</sub> ) Sensor .....	219
8.2.7 PM10 Sensor .....	220
8.2.8 PM2.5 Sensor .....	220
8.2.9 Noise Sensor.....	221
8.3 Fleet Tracking Unit .....	221
8.4 Waste Water Sensor .....	222
8.4.1 Multi-Parameter Smart Controller (Micro-Station) for COD, BOD, TOC, TSS, pH, DO, NH4-N, Temperature, Oil and Grease parameters.....	222
8.4.2 Sensor Probe for BOD/COD/TOC/TSS.....	224
8.4.3 Sensor Probe for DO (Dissolved Oxygen).....	225
8.4.4 Sensor Probe for Nitrate (NO <sub>3</sub> -N) and Ammonical Nitrogen (NH4-N).....	226
8.4.5 Sensor Probe for pH and Temperature .....	228
8.4.6 Probe for Oil & Grease Analyser (Open Channel, Floating Type).....	229
8.4.7 IEG with integrated 3G/4G communication capabilities with Cable and Other Accessories.....	230
8.4.8 Field Enclosure / Panels for Waste water Quality Monitoring Stations / Controllers, IEG	231
8.5 Network Backbone.....	233
8.5.1 Electric Meter.....	233
8.5.2 Industrial grade Field Layer-2 FE 8 port POE Switch .....	237
8.5.3 Industrial grade Field Layer-2 FE 16 port POE Switch.....	239
8.5.4 Junction Box 1 KVA (Outdoor Utility Cabinet).....	239
8.5.5 Junction Box 2 KVA (Outdoor Utility Cabinet).....	241
8.6 Data Centre.....	243
8.6.1 Surveillance Storage (1300 TB NL SAS Drives Usable Capacity).....	243
8.6.2 SAN Switch .....	244
8.6.3 Unified storage with SAN Switch (125TB for Video and Application Data) .....	245
8.6.4 Blade Servers (Web, Application, Database, Platform Solutions etc.) .....	246

8.6.5	Rack - 42 U with necessary cabling.....	247
8.6.6	Blade Chassis with Switch and virtual KVM .....	247
8.6.7	Internet Router .....	249
8.6.8	Core Router.....	252
8.6.9	Spine Switch.....	254
8.6.10	Leaf (TOR) Switch .....	256
8.6.11	Internet Firewall.....	258
8.6.12	Internal Firewall .....	261
8.6.13	Web Security Appliance.....	264
8.6.14	L3 Switch.....	268
8.6.15	24-Port PoE GE layer 2 Switch.....	270
8.6.16	12-Port Layer 3 10G Switch (For Interconnecting).....	271
8.6.17	Authentication, Authorization and Accounting (AAA) Specification).....	273
8.6.18	Network Behaviour Analysis .....	276
8.6.19	SMS Gateway .....	278
8.6.20	Fabric Controller.....	279
8.7	Generic IT Hardware .....	282
8.7.1	Keyboard and Joystick .....	282
8.7.2	Video Wall.....	283
8.7.3	PC – ICCC.....	284
8.7.4	PC – DC & Help desk .....	284
8.7.5	Printer.....	285
8.7.6	Desktop.....	285
8.7.7	IP Camera Surveillance .....	286
8.8	Non - IT Hardware .....	287
8.8.1	Fire Alarm System.....	287
8.8.2	Rodent Repellent System.....	290
8.8.3	Air-conditioned 2 Ton.....	290
8.8.4	Centralized Cooling System.....	291
8.8.5	HVAC – PAC .....	292
8.8.6	Transformer .....	296
8.8.7	LT Distribution Panel .....	304
8.8.8	Lighting .....	306
8.8.9	Diesel Generator 250KVA .....	307
8.8.10	UPS 60 KVA .....	309
8.8.11	UPS 20 KVA .....	310

8.8.12 Projector .....	311
8.9 Helpdesk Hardware.....	312
8.9.1 IP phone.....	312
8.9.2 IP PBX (Call Control System).....	313
8.9.3 Soft Phone.....	314
8.9.4 IVR & ACD .....	317
8.10 Variable Message Display (VMD) Board.....	319
9. Technical Specifications Software .....	320
9.1 Integrated Command Control Centre .....	320
9.1.1 Video wall management Software .....	320
9.2 Data Centre - Software.....	321
9.2.1 Integrated Command & Control Centre (ICCC) Platform.....	321
9.2.2 Enterprise Content Management System / Document Management System .....	331
9.2.3 EMS and Network Monitoring System .....	334
9.2.4 Identity Access Management Software (IAM) .....	340
9.2.5 Directory Services.....	340
9.2.6 Backup Software .....	340
9.2.7 Antivirus Solutions.....	341
9.2.8 Automation and Orchestration Solution .....	342
9.2.9 Compute Virtualization Solution (Compute).....	342
9.2.10 Network and Security Virtualization .....	344
9.2.11 Building Management System .....	345
9.2.12 Central Environment System .....	347
9.2.13 Video Management System.....	348
9.2.14 Video Analytics.....	352
9.2.15 Face Recognition System Software .....	354
9.2.16 ANPR Software .....	356
9.2.17 Body Camera Software License.....	360
9.2.18 Public Announcement Software License .....	361
9.2.19 Fleet Tracking Software .....	363
9.2.20 OWQMS Web Application .....	364
9.2.21 Anti-Virus Solution.....	365
9.2.22 Web based Helpdesk & Incident Management Software with Application / Platform / OS Licenses .....	366
9.3 Disaster Recovery Infrastructure Software .....	379
10. Annexure I: Indicative Bill of Material.....	Error! Bookmark not defined.

11.	Annexure II: IP Camera Locations.....	381
12.	Annexure III: Air Quality Monitoring Station Locations .....	409
13.	Annexure IV: Water Quality Analyzer .....	409
14.	Annexure V: Manpower Requirements .....	410
14.1	Manpower/Resource Requirements for Operations & Maintenance of Smart Solutions in Amritsar City.....	410
14.1.1	Project Manager - IT Infrastructure.....	410
14.1.2	Technical Lead.....	411
14.1.3	System Admin - L2.....	411
14.1.4	Network Admin - L2.....	412
14.1.5	Security Specialist - L2 .....	412
14.1.6	DB Administrator - L2 .....	412
14.1.7	Video Analyst / IP camera Surveillance Expert - L3 .....	413
14.1.8	Software Developer (Full Stack Developer) - L3.....	413
14.1.9	Support Engineer – L1.....	414
14.1.10	Electrical Maintenance Engineer.....	414
14.1.11	HVAC Technician.....	414
14.1.12	EMS Support Engineer – L2 .....	415
14.1.13	BMS Support Engineer – L2 .....	415
14.1.14	Helpdesk Staff .....	415
14.1.15	Security Staff .....	416
15.	Annexure VI: Location Details of Public Address System.....	417
16.	Annexure VII: Location Details of Public Address System.....	418
17.	Annexure VIII: Indicative ICCC Room Layout.....	420

## 1. Project Background

### 1.1 Smart City Mission

Smart City Mission was launched by Hon'ble Prime Minister of India in June 2015. The Smart City Mission envisages interventions in across 98 cities in the country over a period of 5 years i.e. Mission Period 2015-2020. Government of India will give a Grant of Rs.100 Crore per city for 5 years. Smart cities Selection is through competition after evaluation of the Smart City Proposals (SCP) prepared through Intense Citizen Consultation by the cities by a Panel of Experts put in place by MoUD, GoI.

The strategic components of Area-based Development (ABD) in the Smart Cities Mission are city improvement (retrofitting), city renewal (redevelopment) and city extension (Greenfield development) plus a Pan-city initiative in which Smart Solutions are applied covering larger parts of the city.

The Mission aims to development, design, build and operationalize smart and innovative solutions across core city infrastructures including:

- Adequate water supply and Assured electricity supply.
- Sanitation, including solid waste management
- Efficient urban mobility and public transport
- Affordable housing, especially for the poor
- Robust IT connectivity and digitalization
- Good governance, especially e-governance and citizen participation
- Sustainable environment
- Safety and security of citizens, particularly women, children and the elderly
- Health and education

### 1.2 Smart Cities in Punjab

Following cities of Punjab are under Smart Cities Mission of Ministry of Urban Development (MoUD), Govt. of India:

- Amritsar
- Ludhiana
- Jalandhar

Name of the City	Brief Background
Amritsar Smart City	Amritsar is the historically also known as Ramdaspur and colloquially as Ambarsar, in north-western India is major trading and commercial centre in the Majha region of the Indian state of Punjab. The city is situated 217 km northwest of state capital Chandigarh and 455 km northwest of Delhi. It is near Pakistan, with the Wagah Border being only 28 km away. The closest major city is Lahore, the second largest city in Pakistan, located 50 km to the west.

Name of the City	Brief Background
	<p>Amritsar is a major spiritual and cultural centre for Sikh religion. Amritsar is home to the Harmandir Sahib (commonly known as the Golden Temple), which is one of the India's biggest tourist's attraction. More than 2.5 crore tourists visited Amritsar in year 2016, wherein apart from the Golden Temple, Wagah Border and other historic places attract tourists throughout the year.</p> <p>Walled city area (&gt;950 acres) is selected for Retrofit-Redevelopment through desk research, analysis, meetings with public representatives, prominent citizens and citizen's engagement. The total area of walled city is of the order of 350 hectares, approximately of about 2.4 Km. in length and 1.5 Km. of width. It houses nearly 1/6th of the population of district Amritsar.</p>
Ludhiana Smart City	<p>Ludhiana is the largest city in the Punjab with an area of 310 sq.km and an estimated population of 1,618,879 as of the 2011 census. It is an industrial centre of northern India, and was referred to as India's Manchester by the BBC. The city stands on the Sutlej River's old bank, 13 kilometres south of its present course. Ludhiana is located 107 kilometres west of the state capital Chandigarh on NH 95 and is centrally located on National Highway 1, which runs from the Indian capital New Delhi to Amritsar. It is also located 315 km north of Delhi and 142 km southeast of Amritsar.</p> <p>AREA BASED DEVELOPMENT (ABD) Area Selected- Ferozepur Road Area: Rose Garden, Ghumar Mandi, Bhaibala Chowk (retrofitting) - Population (38,000 - projected 2017) - Area (790 acres)</p>
Jalandhar Smart City	<p>Jalandhar is the leading sports &amp; manufacturing hub in Asia. Jalandhar is the oldest inhabited major city in the Indian state of Punjab. In recent times the city has undergone rapid urbanisation and has developed into a highly industrialised centre of commerce. Jalandhar is 144 km northwest of Chandigarh, the state capital of Punjab and Haryana</p> <p>AREA BASED DEVELOPMENT (ABD) Area Selected Burlton Park &amp; Adjoining Area - Population (73,260) - Area (1010 acres)</p>

### 1.3 Project Background

With the objective to usher Technology-led Transformation which would help in transforming Amritsar into a Safe and Smart sustainable City. ASCL has identified below mentioned identified ICT led Smart City Initiatives:

#### Area Based Development Projects<sup>1</sup>

Area Based Development Project Components as per Smart City Proposal		
S. No.	Module Name	Project Components
1.	Transport and Mobility Module	Road Development
2.		No Parking Zones with Smart Parking
3.		Pedestrian Friendly Roads
4.		Real Time Air Monitoring
5.		Last Mile connectivity with e-Rickshaw
6.		Cycle Sharing System
7.	Assured Electricity Supply System	Smart Power Grid for 24x7 Un-Interrupted Power Supply & Improved Efficiency
8.		Micro Grid Monitoring by replacing Existing Meters with Smart Meters
9.		Smart LED Street Lights
10.		Undergrounding of Electrical Overhead Cables to improve Streetscapes
11.	Water Supply, Waste Water and Sanitation	24x7 Water Supply System with SCADA Sensors
12.		100% Smart Water Metering
13.		Reuse of Recycled Waste Water
14.		Strom Water Drainage with Channelization
15.	Solid Waste Management	100% Collection and Segregation
16.		Smart Garbage Bins
17.		Mechanical Sweeping
18.		Economical Transportation and Scientific Disposal of Waste
19.	Open Space and Visibility Improvement	Re-inventing available hierarchy of Urban Spaces (60 No's) as attractive Public spaces for Recreational Areas

<sup>1</sup> Projects identified in the Smart City Proposal (SCP)

Area Based Development Project Components as per Smart City Proposal		
S. No.	Module Name	Project Components
20.	E-Governance and Citizen Services	Re-inventing available Spaces along with Circular Roads as Attractive Public Spaces for Recreational Areas
21.		Conversion of Sakatri & Gol Bagh into thematic Cultural Destination
22.		Construction of Tourist Assistance Centre
23.		Creating Public Squares as Open Theatres
24.		Refurbishment of Peripheral wall of walled city
25.	E-Governance and Citizen Services	Development of Smart Mobile App for Municipal Services for the Citizens
26.		Cameras with fully Equipped Operation Control Rooms for Walled City Area
27.		Mobile Based Exploratory App for Ease of Tourists
28.	Re-Development of Public Amenities	Re-development of Town Hall into Socio-Cultural Re-creational Centre
29.		Decongestion of walled city whole Sale Trade Cluster to City Periphery
30.		Improved Green Cover in Walled City
31.		Innovative Use of Open Spaces
32.	Relocation of polluting Dense Urban Clusters from Core Area	Moving polluting wholesale Clusters Outside the Walled City
33.		Skill Development Centers to promote brand "Amritsari"
34.		Affordable Housing Units on Mix Use Development

### Pan City Solution Projects<sup>2</sup>

Pan City Project Components as per Smart City Proposal		
S. No.	Module Name	Project Components
1.	Traffic and Mobility	Intelligent Traffic Management System

<sup>2</sup> Projects identified in the Smart City Proposal (SCP)

Pan City Project Components as per Smart City Proposal		
S. No.	Module Name	Project Components
2.	Intelligent Solid Waste Management	IP Based Video Surveillance System
3.		Variable message Sign Board
4.		Intelligent Parking
5.		E-Rickshaws
6.		BRTS with Disabled friendly buses
7.		Smart Street lighting
8.		Cycle Tracks and NMT
9.		Door to Door Collection System with 24x7 Control System
10.	E-Governance	Segregation at Source
11.		Intelligent Smart Bins
12.		Waste Transport Routing Map
13.		GPS based Vehicle Tracking System
14.		Weight Bridge Facility
15.		Waste to Energy Sites with ZERO Waste Status
16.		Command and Control Centre
17.	Piped Local Gas Network Distribution System	Public Grievance Redressal through Online Platform
18.		Tourist Destinations Through One Single Application
19.		Piped Gas network for Household and Commercial usages

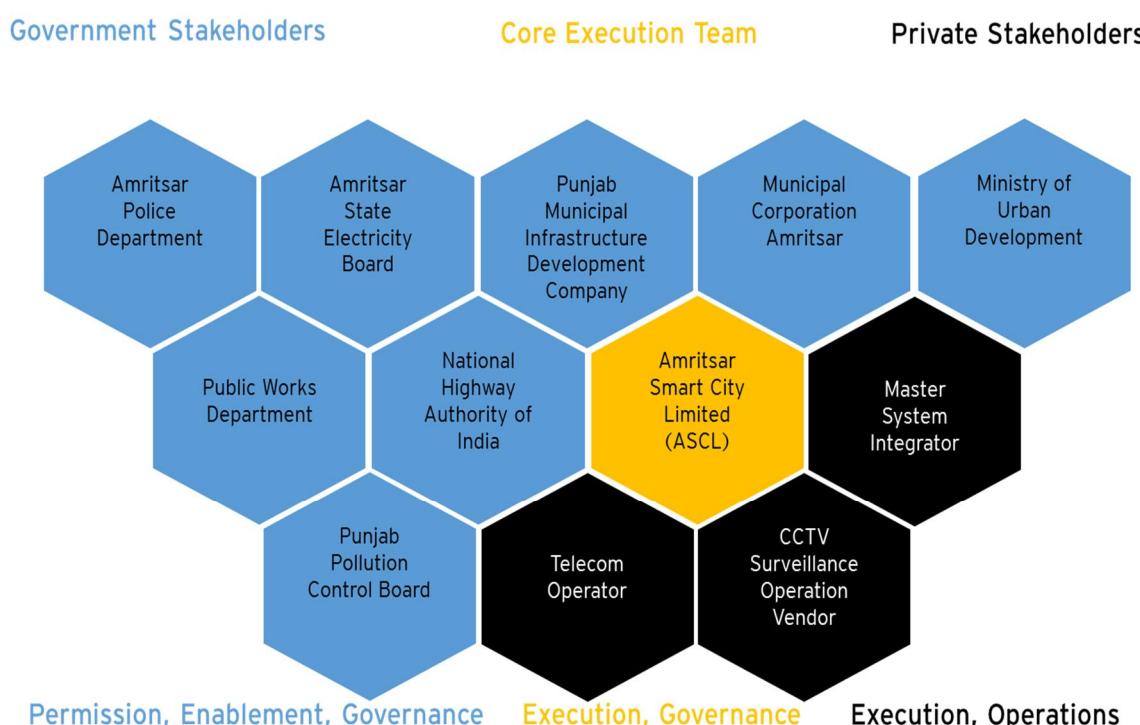
#### 1.4 Project Implementation Phase

S. No.	Project Description	Phase
1.	City Surveillance	Phase I
2.	Environment Sensor	Phase I
3.	Integrated Command and Control Centre	Phase I
4.	Fiber Optic Network (Lease)	Phase I
5.	Public Wi-Fi Network	Phase I
6.	Solid Waste Management	Phase I
7.	Integrated Traffic Management System	Phase II and Beyond
9.	Tourist Destinations Through One Single Application	Phase II and Beyond

S. No.	Project Description	Phase
10.	Variable message Sign Board	Phase II and Beyond
11.	Development of Smart Mobile App for Municipal Services for the Citizens	Phase II and Beyond
11.	100% Smart Water Metering	Phase II and Beyond
12.	Micro Grid Monitoring by replacing Existing Meters with Smart Meters	Phase II and Beyond
13.	Last Mile connectivity with e-Rickshaw	Phase II and Beyond
14.	E-Governance for general citizen	Phase II and Beyond

### 1.5 Project Stakeholders and their roles

The project envisages involvement of multiple stakeholders; some of them would be common for all the smart city solutions while some of them would be solution specific. The snapshot of key stakeholders and their high-level roles are presented below:



S. No	Stake Holder	Roles & Responsibilities
1.	Amritsar Smart City limited	<ul style="list-style-type: none"> <li>To provide overall guidance and approach for implementation &amp; execution of the project.</li> <li>To Monitor the project on routine basis and take critical decisions</li> <li>Provide acceptance of all Solutions implemented by MSI</li> <li>To Provide requirements relating to the project</li> <li>Acceptance of all Solutions implemented by MSI</li> <li>To Provide requisite approvals like site preparation for installation of networks ducts and provisioning permission for right-of-way</li> </ul>

S. No	Stake Holder	Roles & Responsibilities
		<ul style="list-style-type: none"> <li>• To provide network and bandwidth requirement for implementation of all identified solutions</li> <li>• To assist in collation and identification about information pertaining to locations regarding implementation of CCTV Surveillance, Environment sensor, Water Quality Analyzer and Network Connectivity</li> </ul>
2.	Departments / Agencies (Government Stakeholders)	<ul style="list-style-type: none"> <li>• Provide necessary information pertaining to design, development and implementation of Integrated Command and Control Centre and CCTV Camera.</li> <li>• Support and coordination for implementation of various smart city initiatives at Amritsar</li> <li>• Provide requisite approvals as and when required</li> <li>• Participate in the project implementation and provide necessary feedback</li> </ul>
3.	Amritsar Police Department	<ul style="list-style-type: none"> <li>• To provide inputs on critical infrastructure &amp; rules etc.</li> <li>• To deploy resources at Command and Control Centre</li> <li>• To inform and share the identified locations for the installation of cameras</li> <li>• To inform type of cameras, number of cameras and lat/long details etc.</li> <li>• To be trained on the new system</li> </ul>
4.	Punjab Pollution control Board	<ul style="list-style-type: none"> <li>• To provide inputs on critical infrastructure &amp; rules etc.</li> <li>• To inform and share the identified locations for the installation of Water Sensors and Water Quality Analyzer</li> <li>• To be trained on the new system</li> </ul>
5.	Citizens	<ul style="list-style-type: none"> <li>• Provide feedback on their ideas and apprehensions on the systems</li> </ul>

It is endeavoured that future smart city initiatives can leverage on this foundation components to provide services to citizens of Amritsar.

## 2. City Surveillance

### 2.1 Existing Solutions (As-Is Study)

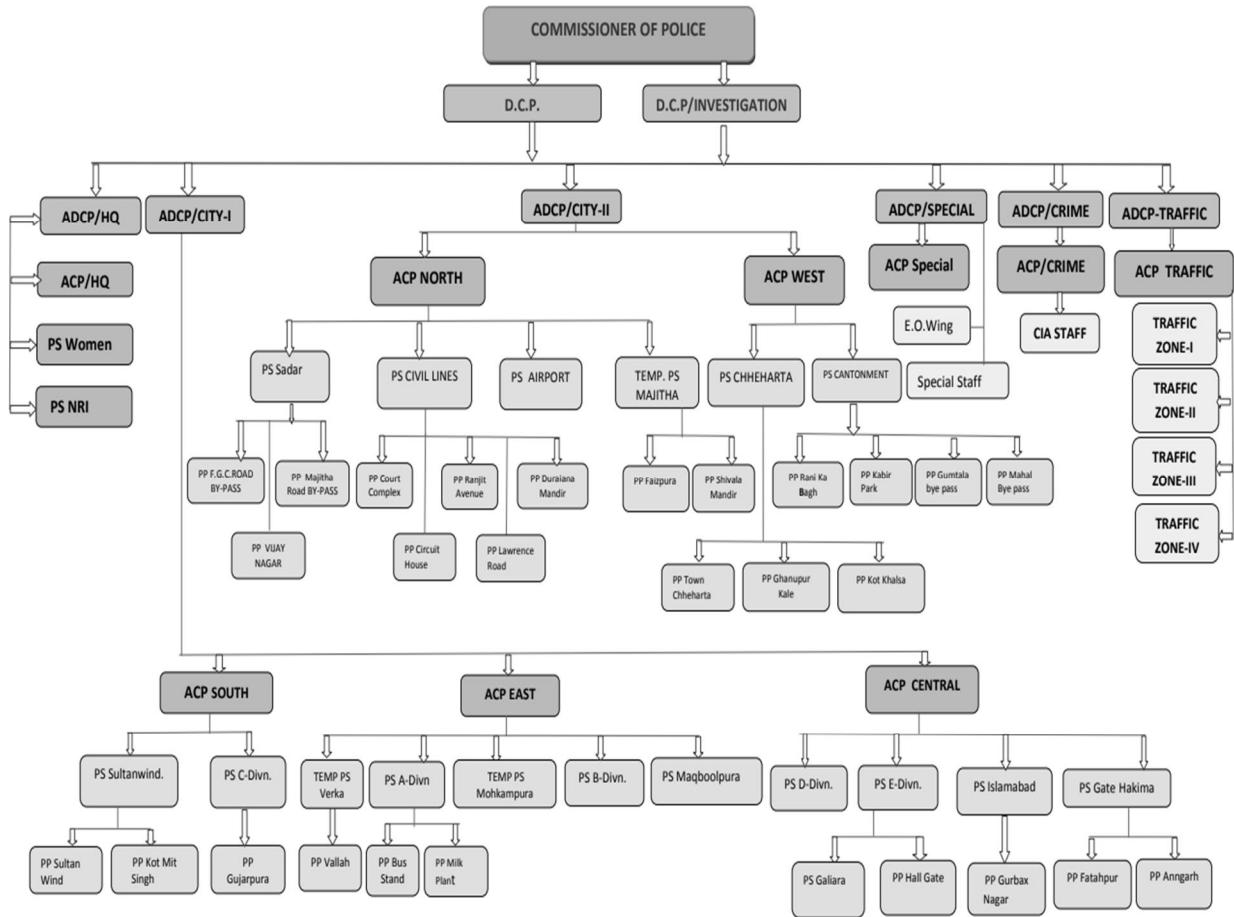
#### 2.1.1 Amritsar Police

Punjab Police has had an extremely proud history and the legend of keeping duty before self. Even before Independence, Punjab Police had a name in the country for effective policing and this has been continuously improving through the personal examples of its leadership supported by great traditions, discipline, and highly professional attitude.

The emergence of Punjab Police as a separate organization is a post 1861 development, which took place after the British annexation of Punjab in 1849. In about 150 years of its existence, the police force in the state has faced many difficult phases. The onus of handling law and order has always been a challenge before the police mainly because of the inherent martial traditions prevailing in the state.

Setting up of the Police Training School at Phillaur in 1891, and later the introduction of finger print section has been among the achievements of the Punjab Police.

Organization chart of Amritsar Police department are shown in the below hierarchy



### 2.1.2 Existing Surveillance Camera Location Details

There are 202 cameras (200 Fixed and 2 PTZ) which are currently installed at 40 different locations across the Amritsar City. These cameras are monitored through 6 isolated control centres by Amritsar Police.

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

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
4.		Lawrence cross Road	6	-	1	-
				-	1	-
				-	1	-
				1	-	-
				1	-	-
				1	-	-
		DAV College / Lawrence Road	3	1	-	-
				1	-	-
				1	-	-
6.		Purani Chungi	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
7.		Thasundera singh Chowk	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
8.		Mall road School	3	1	-	-
				1	-	-
				1	-	-
9.		Trillium Mall Junction	3	1	-	-
				1	-	-
				1	-	-
10.		Ratan singh Chowk	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
11.		ESI Cross Road	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
12.		Fatehgarh Chudiyanghar Circle	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
13.		88 Feet Road entry	4	-	1	-
				-	1	-
				-	1	-
				-	1	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
14.		88 Feet Exit	4	-	1	-
				-	1	-
				-	1	-
				-	1	-
15.		Kabir Marg	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
16.		Verka By-pass	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				-	1	-
17.		Majitha By-pass	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
18.		Makhan Restaurant Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
19.		Crystal Chowk	5	1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
20.	Civil Line Police Station	4SS Chowk	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
21.		Joshi Colony Market	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
22.		Circular Road (opposite TSPCL office)	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				-	1	-
23.		Musta Chowk (Bagh chowk)	5	1	-	-
				1	-	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
24.		Gala Mala Marg	5	1	-	-
				1	-	-
				1	-	-
25.		Gopal Mandir Chowk	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
26.		Hussain Pura Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
27.		Kichlu Chowk	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
28.		District Shopping Centre	7	1	-	-
				1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	-	1
				-	-	-
29.	Suvidha Centre	C - Block market	6	1	-	-
				1	-	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
30.		Green Avenue Market	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
31.		Amrit nal Bagh	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				-	1	-

S. No.	Existing Command Centre	Location of the Cameras	Camera Quantity (Nos.)	Camera Type		
				2 MP	1MP	2 MP PTZ
32.		Gumtala By-pass	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
33.		Railway Station entry point	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
34.	ADCP office	Railway Station exit point	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
35.		UCO Bank (or petrol pump)	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
36.		Railway Station entry / exit, B/H	5	1	-	-
				1	-	-
				1	-	-
				1	-	-
				1	-	-
37.		Bhandhari Bridge	6	1	-	-
				1	-	-
				1	-	-
				1	-	-
				-	-	1
				-	1	-
38.	Durgiyana Police Station	Hall Gate	6	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
39.		Durgiyana Mandir (Hathi chowk)	5	-	1	-
				-	1	-
				-	1	-
				-	1	-
				-	1	-
40.		Durgiyana New Entrance	2	1	-	-
				-	1	-
Total				120	80	2

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

### 2.1.3 Existing Infrastructure Details

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

## 2.2 ASCL requirement for Security Surveillance

### 2.2.1 Requirement for Surveillance for Citizen

Protecting citizens and ensuring public safety is one of the topmost priority of any Government. Governments and law enforcement agencies require advanced security solutions to effectively fight threats from activities of terrorism, organized crime, vandalism, burglary, random acts of violence, and all other forms of crime. Video surveillance is a fitting solution to commence the journey of government and law enforcement agencies in implementing advanced security for public safety.

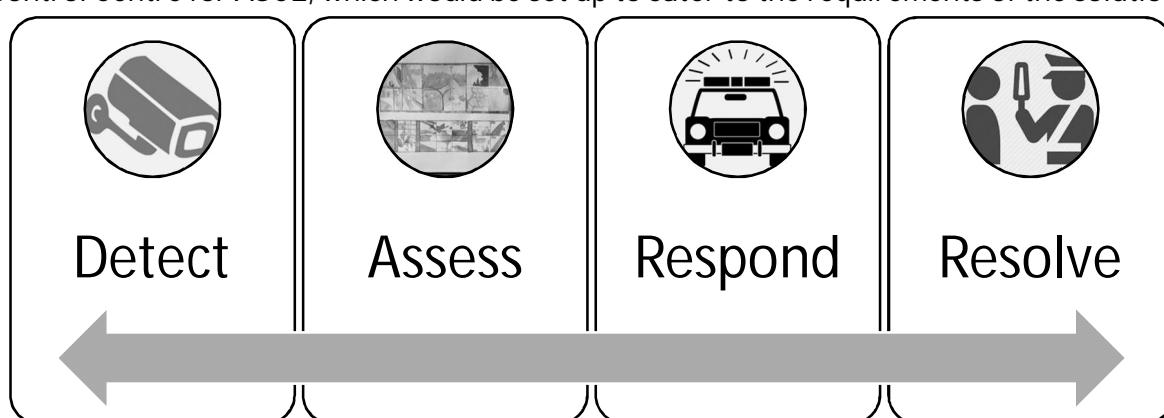
As elaborated in earlier sections, the Vision of Amritsar Smart City specifies building of world-class infrastructure using smart elements. Further, the big picture and envisioned future-state of Amritsar Smart City identifies implementation of infrastructure-intensive smart solutions; Security Surveillance being one of the infrastructure-intensive smart solutions. The envisaged Security Surveillance System is expected to monitor citizens through strategically placed sensors throughout the City, which can collect data regarding many different factors such as crime prevention, object / person identification, and so on. It is also envisaged that the video inputs from few sensors implemented as part of Security Surveillance System can be provided for monitoring civic functions like energy use and waste reduction. The proposed Security Surveillance System can not only facilitate better law enforcement and urban planning, and but also allow all stakeholders of the Smart City Project to tailor their services to requirements and expectation of beneficiaries.

Proposed Security Surveillance System can be designed to accumulate intelligence through data collection strategies key to intelligence-based policing, and through extensive CCTV installations, and crime prediction software. This set-up can aid in significantly improving the type and volume of information that is relied upon by law enforcement authorities when dealing with crimes.

Commissioning of the proposed Security Surveillance System can involve setting up of IP based outdoor security cameras, installed across different locations of strategic importance throughout Amritsar City. The system can have the ability to monitor, detect and record any criminal activities including theft, traffic violations etc.

Video surveillance data from cameras deployed at critical areas can be stored, monitored and analysed at Integrated Command and Control Centre of ASCL.

The servers, storage devices and core network components for computing, processing and storage of data, and analysis can be housed in the Data Centre for Integrated Command and Control Centre for ASCL, which would be set up to cater to the requirements of the solution.



## 2.2.2 Need of Security Surveillance in Amritsar City

The word surveillance came from a French phrase for "watching over" ("sur" means "from above" and "veiller" means "to watch").

Surveillance is monitoring of the behaviour, activities, or other changing information; usually of people, for protecting people. Surveillance is used by governments and law enforcement agencies for intelligence gathering of data, prevention of crime, protection of citizens and for investigation of crime. Following details highlight the need for Security Surveillance system in Amritsar City:

- I. Conventional law enforcement mechanism has not been able to keep pace with rapid urbanization
- II. There has been an asymmetric growth in City population and vehicular traffic
- III. Change in behavioural pattern of crimes
- IV. Increase in traffic violations and related crime
- V. Lack of technology intervention to address all of the above
- VI. Limitation in manpower to address security needs of the city
- VII. Lack of emergency response mechanism

## 2.2.3 Amritsar Police intends to implement a city-wide Security Surveillance system with the following objectives

Traffic Monitoring<sup>3</sup>



<sup>3</sup> <https://www.hindustantimes.com/punjab/fee-row-parents-block-bhandari-bridge-in-amritsar-for-6-hours-cause-traffic-jam/story-FRYVW8H7HkfLHVlmjj3BFP.html>

Crime Surveillance<sup>4</sup>



Post Incident Analysis



Crowd Management<sup>5</sup>



<sup>4</sup> <https://www.amarujala.com/photo-gallery/chandigarh/crime/bathinda-girl-brutally-murdered-by-her-boyfriend-at-his-farm>

<sup>5</sup> <http://www.tribuneindia.com/2011/20110330/aplus.htm>

## 2.3 Air Quality Analyzer Sensor

### 2.3.1 Brief History of Punjab Pollution Control Board

The Punjab Pollution Control Board was constituted in the year 1975 vide Punjab Government Notification No. 6186-BR II (4) 75/24146 dated 30.07.1975, after the enactment of Water (Prevention & Control of Pollution) Act, 1974 to preserve the wholesomeness of water. Subsequently, with the enactment of other environmental laws the responsibility to implement the provisions of such laws was also entrusted to the Punjab Pollution Control Board in the State of Punjab.

### 2.3.2 Details about Punjab Air Laboratory

Ambient Air Quality is monitored at 28 locations including 4 rural area stations in Punjab under National Air Monitoring Programme (NAMP) for 24 hrs. thrice a week. The monitoring of ambient air is carried out in the cities i.e. Patiala, Bathinda, Dera Bassi, Amritsar, Jalandhar, Ludhiana, Khanna, Mandi Gobindgarh Dera Baba Nanak, Batala and Naya Nangal. These stations have been set up for monitoring Respirable Suspended Particulate Matter (PM10), Sulphide dioxide (SO<sub>2</sub>) and oxides of Nitrogen (NO<sub>x</sub>). Four stations have been set up in Rural Areas in village Rasulpur (Dist. Amritsar), Village Gangsar (Distt. Sangrur), Village Himmatpura (Distt. Faridkot) and Village Mukandpur (Dist. S.B.S Nagar) to monitor the impact of burning of agricultural residue on the ambient air quality there which are the first ever stations installed in the country.

The ambient air quality monitoring data of all these stations are being sent to the Central Pollution Control Board through EDB/Excel format regularly by air laboratory. This monitoring is financed by Central Pollution Control Board, New Delhi.

During the year 2013-2014 the Board monitored the Ambient Air Quality by collecting 41480 ambient air samples.

Head office Air Laboratory carries out stack sample monitoring of regional offices Fatehgarh sahib, Patiala, Sangrur, Bathinda, Faridkot & Nodal Office, Mohali.

Eleven nos. laboratories (10 private +1 Govt.) have been recognized by the Board and work concerning approval of laboratories is carried out by air lab. The laboratories approved by the Board can be perused at the link-Private laboratories approved by the Board.

### 2.3.3 List of Ambient Air Quality Stations (NAMP) in the State of Punjab

S. No.	Name of Station
1.	R.O. Building Amritsar
2.	Vinod Chilling Centre, Amritsar
3.	Golden Temple, Amritsar
4.	Milk Plant, Bathinda
5.	C-Pyte, Dera Baba Nanak
6.	Winsome Yarn Ltd., Barwala Road, Dera Bassi
7.	PCPL, Dera Bassi
8.	R.O.Jalandhar
9.	Punjab Maltex, Sports & Sugical Complex, JDR
10.	Focal Point, Jalandhar
11.	MC Tubewell, JDR now Zonal Office, JDR
12.	A.S. Senior Secondary School, Khanna
13.	Markfed, Khanna
14.	Milk Plant, Ludhiana
15.	Rita Sewing Machine/ JBR, Ludhiana
16.	Vishvakarma Chowk, Ludhiana
17.	Zonal Office, Ludhiana
18.	Raj Steel, Mandi Gobindgarh
19.	Modi Oil, Mandi Gobindgarh
20.	United steel, Mandi Gobindgarh
21.	NFL, Naya Nangal
22.	PACL, Naya Nangal
23.	Ceylon Industries, Patiala
24.	Fire Brigade Station, Patiala
25.	R.O Building, Batala

### 2.3.4 List of Ambient Air Quality Stations (NAMP) in the Rural Area of Punjab

S. No.	Name of Station
1.	Gurudwara Gangsar, Vill. Gangsar, Distt. Sangrur
2.	Village .Himmatpura, Distt .Faridkot
3.	Village .Rasulpur, Distt .Amritsar
4.	Village Mukandpur, Distt. SBS Nagar

### 2.3.5 Functions of Punjab Pollution Control Board

#### 2.3.5.1 Pollution Control Regulatory functions

- I. To inspect industrial plants and manufacturing process, sewage or trade effluents, works and plants for the treatment of sewage and trade effluent or any control

equipment, to review plans, specifications or other data relating to plants set up for effluent treatment or air pollution control devices, in connection with the issue consents for installation and operation of industrial plant and to give, such directions to such persons as it may consider necessary to take steps for the prevention and control or abatement of water or air pollution.

- II. To ensure that hazardous wastes generated by the industry are stored and disposed of without any detrimental effect to the environment.

#### *2.3.5.2 Pollution Assessment*

- I. To assess the quality of water of rivers, streams, wells & ambient air in the State & to plan a comprehensive Programme for the prevention, control & abatement of pollution.
- II. Laying Down Standards for Effluent and Emissions
- III. To lay down, modify or annual effluent standards for the sewage and trade effluents and for the quality of receiving waters resulting from the discharge of effluents and for the emissions of air pollutants into the atmosphere from industrial plants and automobiles.
- IV. Research & Development including setting up of the demonstration plants
- V. To encourage, conduct and participate in investigations and research relating to problems of water & air pollution and prevention, control or abatement thereof and to evolve economical and reliable methods of treatment of sewage and trade effluents, having regard to peculiar conditions of soils, climate and water resources of different regions.
- VI. To evolve method of utilization of sewage & trade effluents on land for agricultural purposes.

#### *2.3.5.3 Environment Awareness Programme*

- I. To collect and disseminate information relating to water and air pollution and prevention, control or abatement thereof.
- II. To collaborate with Central Board in organizing the training of persons engaged or to be engaged in program relating to prevention, control or abatement of water and air pollution and to organize mass education programs relating thereto.

#### *2.3.5.4 Advisory Role*

- I. To advise the State Government on any matter concerning the prevention control or abatement of water and air pollution.

#### *2.3.5.5 Establishment Laboratories*

- I. To establish or recognize laboratories for analysing of sample of sewage or trade effluent & air emission into the atmosphere.

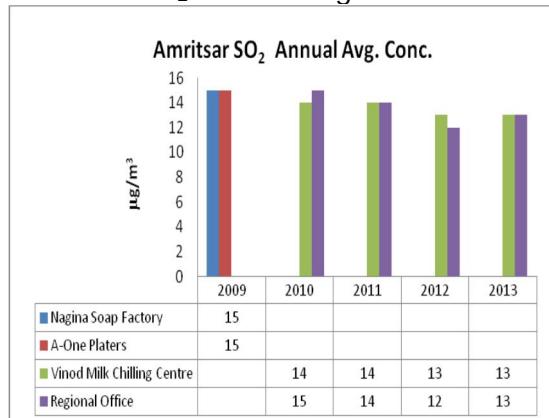
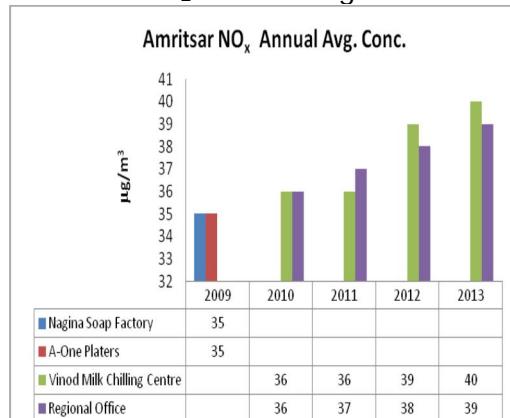
### 2.3.6 Comparative Values of RSPM, SO<sub>2</sub> & NO<sub>x</sub> µg/m<sup>3</sup> for the years 2013-2017

Station Name: M/s Vinod Milk Chilling Centre, Amritsar

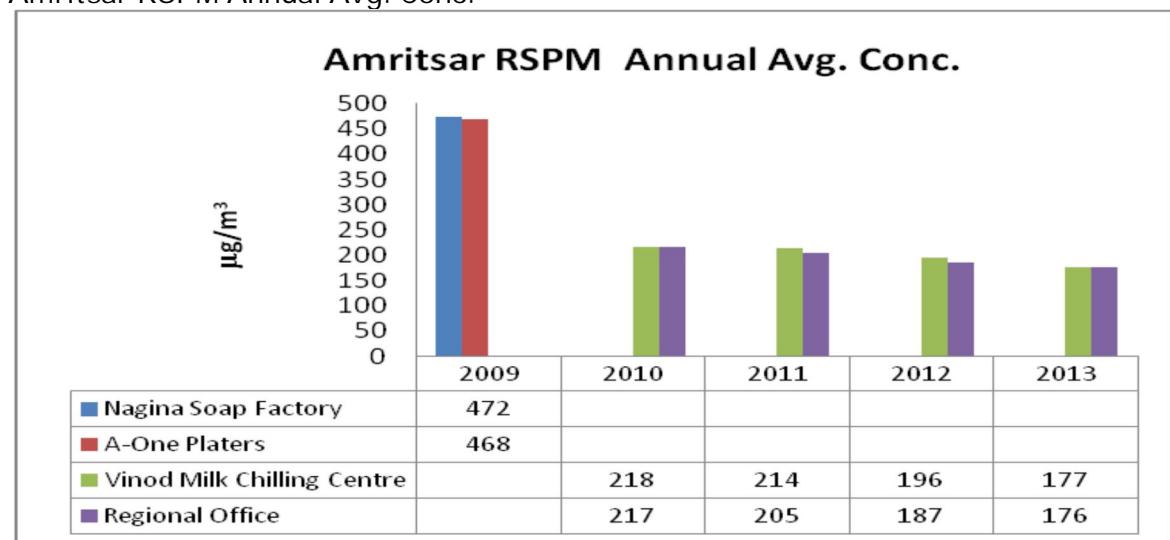
Month	RSPM (µg/m <sup>3</sup> )					NOx (µg/m <sup>3</sup> )					SO <sub>2</sub> (µg/m <sup>3</sup> )				
	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017
January	181	177	204	224	316	38	36	40	40	37	11	13	14	18	13
February	180	170	198	208	213	37	36	39	39	35	12	13	13	17	13
March	182	168	187	218	225	40	35	38	40	34	13	13	12	18	12
April	194	198	211	313	206	41	38	39	40	36	14	14	13	15	12
May	188	215	212	-	167	42	42	39	-	37	14	15	14	-	12
June	171	202	181	205	151	41	43	38	37	35	12	14	13	12	12
July	132	191	178	201	148	39	39	38	36	30	13	13	13	12	10
August	-	182	145	225	180	-	38	37	36	31	-	12	13	12	11
September	-	184	156	261	156	-	40	37	35	29	-	12	13	12	10
October	173	199	161	263	206	39	45	37	37	32	14	14	13	13	12
November	181	191	182	267		40	41	39	36		15	14	15	12	
December	189	202	181	316		41	39	39	37		15	13	15	13	
<b>Annual Avg.</b>	<b>177</b>	<b>190</b>	<b>183</b>	<b>246</b>		<b>40</b>	<b>39</b>	<b>38</b>	<b>38</b>		<b>13</b>	<b>13</b>	<b>13</b>	<b>14</b>	

Station Name: M/s Nagina Soap Factory, Amritsar shifted to Focal Point, R.O.

Month	RSPM (µg/m <sup>3</sup> )					NOx (µg/m <sup>3</sup> )					SO <sub>2</sub> (µg/m <sup>3</sup> )				
	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017
January	178	175	202	246	310	39	38	39	40	41	12	13	14	17	14
February	174	171	195	225	135	36	38	38	38	34	11	13	13	17	12
March	172	170	184	225	198	38	38	37	39	35	12	12	12	18	12
April	205	201	208	239	213	41	39	39	39	36	13	14	14	17	13
May	197	209	210	-	192	42	44	40	-	36	13	14	14	-	12
June	180	199	188	208	-	37	42	39	36	-	12	14	13	14	-
July	160	189	181	128	153	37	41	37	33	28	12	13	13	12	12
August	155	129	141	152	143	36	39	37	32	30	12	12	13	11	12
September	163	178	153	217	140	37	39	38	34	30	13	13	14	11	11
October	169	201	180	211	216	40	48	37	40	34	13	15	13	13	13
November	177	188	194	231		39	42	38	40		14	14	14	13	
December	185	201	190	310		40	41	39	41		14	14	15	14	
<b>Annual Avg.</b>	<b>176</b>	<b>184</b>	<b>186</b>	<b>217</b>		<b>39</b>	<b>41</b>	<b>38</b>	<b>37</b>		<b>13</b>	<b>13</b>	<b>14</b>	<b>14</b>	

Amritsar SO<sub>2</sub> Annual Avg. Conc.Amritsar NO<sub>2</sub> Annual Avg. Conc.

Amritsar RSPM Annual Avg. Conc.



### 2.3.6.1 Monitoring Of Ambient Air Quality & Noise Levels during Festival Days

Festivals in India are celebrated with great festivity, fervour and enthusiasm. Every festival has its own importance at a particular point of time. Public participation is must to keep its fervour. From Dushehra to Diwali, people enjoy these two occasions by using crackers and try to outdo each other. Ambient Air Quality and Noise levels are bound to increase on these days. Suspended Particulate Matter (SPM), Respiratory SPM, Sulphur Dioxide (SO<sub>2</sub>) and Oxides of Nitrogen (NO<sub>x</sub>) and above all, Noise have been widely recognized as major environmental menace in the urban densely populated areas. The annoyance and the consequent adverse health impact of these parameters are well documented. Noise generated from various activities in the cities on these festival days and bursting of high intensity crackers are of serious environmental concern in the Country both from the point of view of public annoyance and public health.

During the period 2013-2014, the Board conducted a study about the impact of Diwali day celebration on the environment particularly on the quality of air with respect to the suspended particulate matter (SPM), obnoxious gases like nitrogen oxides (NO<sub>x</sub>), sulphur dioxides (SO<sub>2</sub>) and high noise levels.

Sulphur Dioxide (SO<sub>2</sub>) and Nitrogen Oxides (NO<sub>x</sub>) samples were collected in each day for 24 hrs. on a 4 hourly basis as per Punjab Pollution Control Board, timings for the NAAQM stations in residential, commercial and sensitive areas in Ludhiana, Jalandhar, Amritsar, Patiala and Mandi Gobindgarh. Noise was monitored during Diwali days i.e. for 6 hrs. (18.00 hours to 24.00 hours) on an hourly average basis at night when the bursting of crackers is expected.

Ambient Air Quality Monitoring 24 Hourly Average Values of RSPM, SO<sub>2</sub>& NO<sub>x</sub> ( $\mu\text{g}/\text{m}^3$ )

<b>Residential Area</b>					
	<b>Mandi Gobindgarh</b>	<b>Patiala</b>	<b>Jalandhar</b>	<b>Ludhiana</b>	<b>Amritsar</b>
<b>RSPM</b>					
Normal Day	154	115	210	240	199
Diwali Day	220	244	305	206	345
<b>SO<sub>2</sub></b>					
Normal Day	6	4	16	12	11
Diwali Day	18	10	30	22	19
<b>NO<sub>x</sub></b>					
Normal Day	19	15	28	26	33
Diwali Day	38	22	34	40	38

Ambient Air Quality Monitoring 24 Hourly Average Values of RSPM, SO<sub>2</sub>& NO<sub>x</sub> ( $\mu\text{g}/\text{m}^3$ )

<b>Sensitive Area</b>					
	<b>Mandi Gobindgarh</b>	<b>Patiala</b>	<b>Jalandhar</b>	<b>Ludhiana</b>	<b>Amritsar</b>
<b>RSPM</b>					
Normal Day	120	110	181	229	192
Diwali Day	206	142	196	308	350
<b>SO<sub>2</sub></b>					
Normal Day	6	4	17	10	12
Diwali Day	12	6	20	15	18
<b>NO<sub>x</sub></b>					
Normal Day	14	12	27	25	32
Diwali Day	26	18	32	32	41

Ambient Air Quality Monitoring 24 Hourly Average Values of RSPM, SO<sub>2</sub> & NO<sub>x</sub> ( $\mu\text{g}/\text{m}^3$ )

Commercial Area					
	Mandi Gobindgarh	Patiala	Jalandhar	Ludhiana	Amritsar
<b>RSPM</b>					
Normal Day	172	123	232	263	223
Diwali Day	250	196	270	549	370
<b>SO<sub>2</sub></b>					
Normal Day	7	5	17	15	11
Diwali Day	18	9	21	18	20
<b>NO<sub>x</sub></b>					
Normal Day	22	14	28	29	34
Diwali Day	32	20	34	46	44

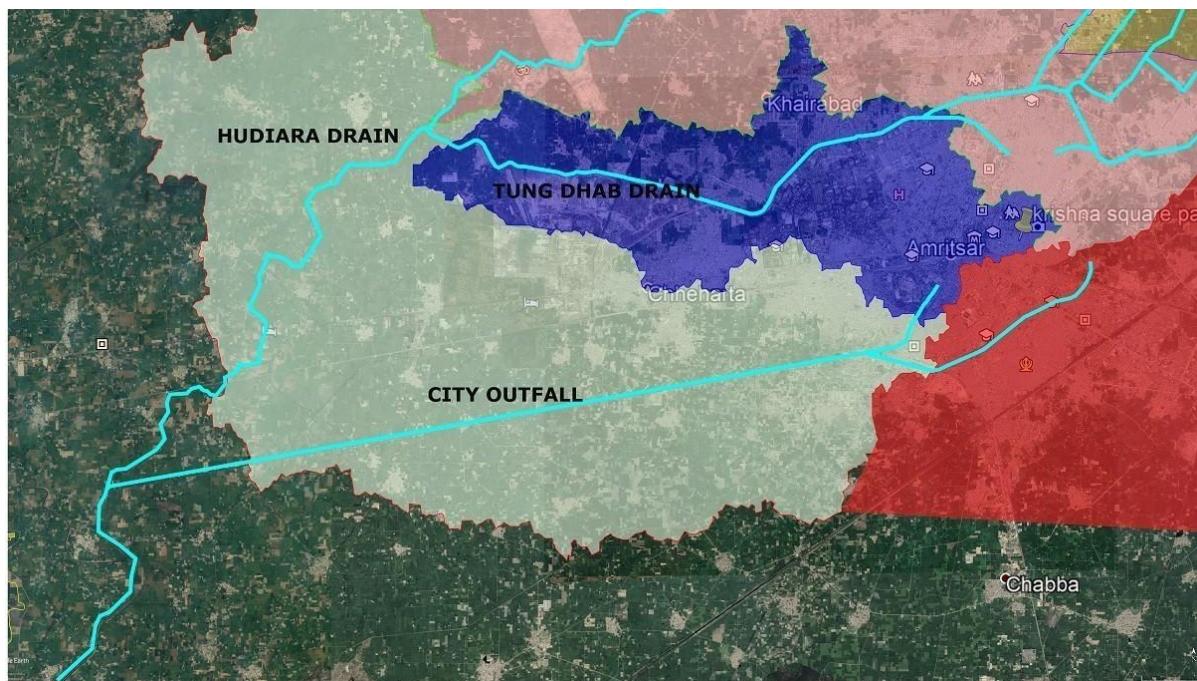
## 2.4 Online Waste-Water Quality Management System for Drainage Canals in Amritsar City

### 2.4.1 Overview

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

- I. Tung Dhab drain
- II. City Outfall drain

The overall drainage system of the city of Amritsar has been presented in below figure



#### 2.4.1.1 Tungdhab Drain

The Tungdhab drain flowing in the northern side of Amritsar city along the Northern Bypass is an important drain originating from north east of the city and finally merging with Hudiara drain flowing in the west of Amritsar LPA. Along its course, it covers many areas/villages such as Pandori, Verka, Othian, Khan Kot, KotMit Singh, Sultanwind, etc. Tungdhab drain is also carrying untreated industrial and sewage effluents and other waste materials, dense weeds, shrubs, silts & mud and is extremely polluted. The flow of drain is moderately high in its downstream side and along its course, spreads strong odour and nuisance towards concerned residential areas within the LPA. As per visual observations, colour of the water is brick red having strong odour with high turbidity level.

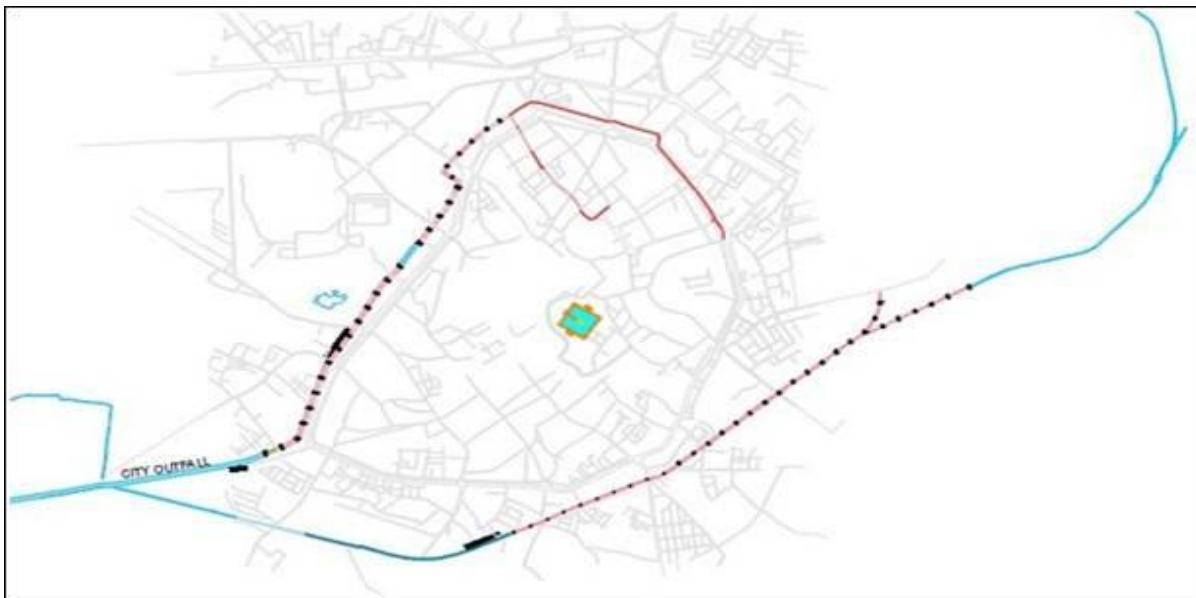


#### 2.4.1.2 City Outfall Drain

The walled city falls under the catchment of city outfall drain as highlighted in below figure. As seen the figure, there are two drain flowing around the walled city of the Amritsar town

- I. Drain starting from city centre passing through old Sabji Mandi, Durgiana Mandir, and Hindustan Basti up to city outfall drain.
- II. Drain starting from Amritsar Jalandhar Railway line passing through East Mohan Nagar, Tarn Taran road Gujjar pura up to city out fall drain.

The drains before discharging into City outfall is being maintained by Municipal Corporation of Amritsar



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

- I. Monitoring of drainage water quality from City Operation Centre of ICCC
- II. Monitoring the Quality of effluent treated and processing at the inlet and discharge of each drain (Tung Dhab and City Outfall)
- III. Measure waste water quality parameters like BOD, COD, DO, TSS, NH4-N, PH , Temperature and Oil & Grease in Tung Dhab and City Outfall Drain
- IV. Integrate data with State and Central Pollution control websites and databases

## 2.5 Communication Network

### 2.5.1 Geographical Scope

Amritsar is a city in north-western India which is the administrative headquarters of the Amritsar district - located in the Majha region of the Indian state of Punjab. It is located at the coordinate  $31.6340^{\circ}$  N  $74.8723^{\circ}$  E. The city is situated 217 km (135 mi) northwest of state capital Chandigarh and 455 km (283 miles) northwest of New Delhi, the national capital. It is near Pakistan, with the Wagah Border being only 28 km (17.4 mi) away. Amritsar Municipal Corporation is divided into 5 Tehsils which are further divided into 4 Sub-Tehsils and 9 blocks.

### 2.5.2 Existing Network Backbone

There are multiple internet service providers in Amritsar city who own Fibre and cable network backbone. Some of the service providers that are operating in Amritsar are BSNL, Airtel, Reliance, Fastway and Connect broadband etc., who intend to provide their network and services for smart city solutions as required by ASCL.

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

## 2.6 Integrated Command Control Centre

### 2.6.1 IT Enablement of Emergency Systems in Amritsar

The Amritsar Police department – City, Rural and Traffic have static webpage, provided basic information about the Amritsar police department with contact details of the key persons. The web features analysis summary of Amritsar police department is given below.

S. No.	Control Room	Web	Online Complaints form	Email	WhatsApp	Face book	Twitter	Toll Free Number
1.	Amritsar City	Yes	Yes	Yes	No	No	No	Yes
2.	Amritsar Rural	Yes	Yes	Yes	No	No	No	Yes
3.	Amritsar Traffic	Yes	Yes	Yes	No	No	No	Yes

The list of the Information technology interventions are available in the Police control room are given below in the below table.

S. No.	Features / Facility	Available (Yes/No)	In Use (Yes/No)
1.	Call distribution system	Yes	No
2.	Call incident management system	Yes	No
3.	Vehicle tracking system	Yes	No
4.	Voice Recording	Yes	No
5.	MDT in the system	No	No
6.	Call takers available	Yes	Yes
7.	Dispatchers	Yes	Yes
8.	Standard operation Procedures	Yes	No

### 2.6.2 Ambulance – Dial 108

A centralised call taker and dispatch facility is established in Amritsar for the state of Punjab. 22 Ambulances are allocated for the Amritsar city. These 22 ambulance are stationed at 22 locations earmarked for them. These ambulances are used for transportation of needy persons to the nearest Public Health Centre or Government Hospital or transfer of patients to the PGIMS in Chandigarh. Currently these vehicles do not have Mobile device terminal, communication is established using mobile phones. GPS are not available in the vehicles.

### 2.6.3 Fire

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

Summary of the IT interventions of police, fire and ambulance control rooms

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

### 2.6.4 Dial 112 – Project in Amritsar

As per the guidelines of the MHA, the Government of Punjab is in the process of implementing Dial 112 project in the state. Police department is identified as the nodal agency to implement the project across the state. The objective of project is to integrate the Police, Fire, and Ambulance in the State with a single emergency number across the state. The project is envisaged in the model of 911 in United States of America.

The Police Department is identified as the nodal agency for implementing this project. The project shall be implemented by CDAC across the state. A centralised call taker facility with twelve decentralised dispatch centres has been planned across the state. The centralised call centre shall be established in Mohali with 150 seating capacity and 12 dispatch centre across Punjab. MPLS connectivity shall be used to connect the call taker centre with the 12 dispatch centres. The solutions shall have Geographical Information System (GIS), Computer Aided Dispatch (CAD) system and Mobile Device Terminals.

A dispatch centre in the Taran is being planned for the Amritsar city under Dial 112 project.

A command and control centre exclusively for Surveillance and Municipal functions is being planned as part of the Amritsar Smart city Project.

### 3. Scope of Work

#### 3.1 General Scope of Work

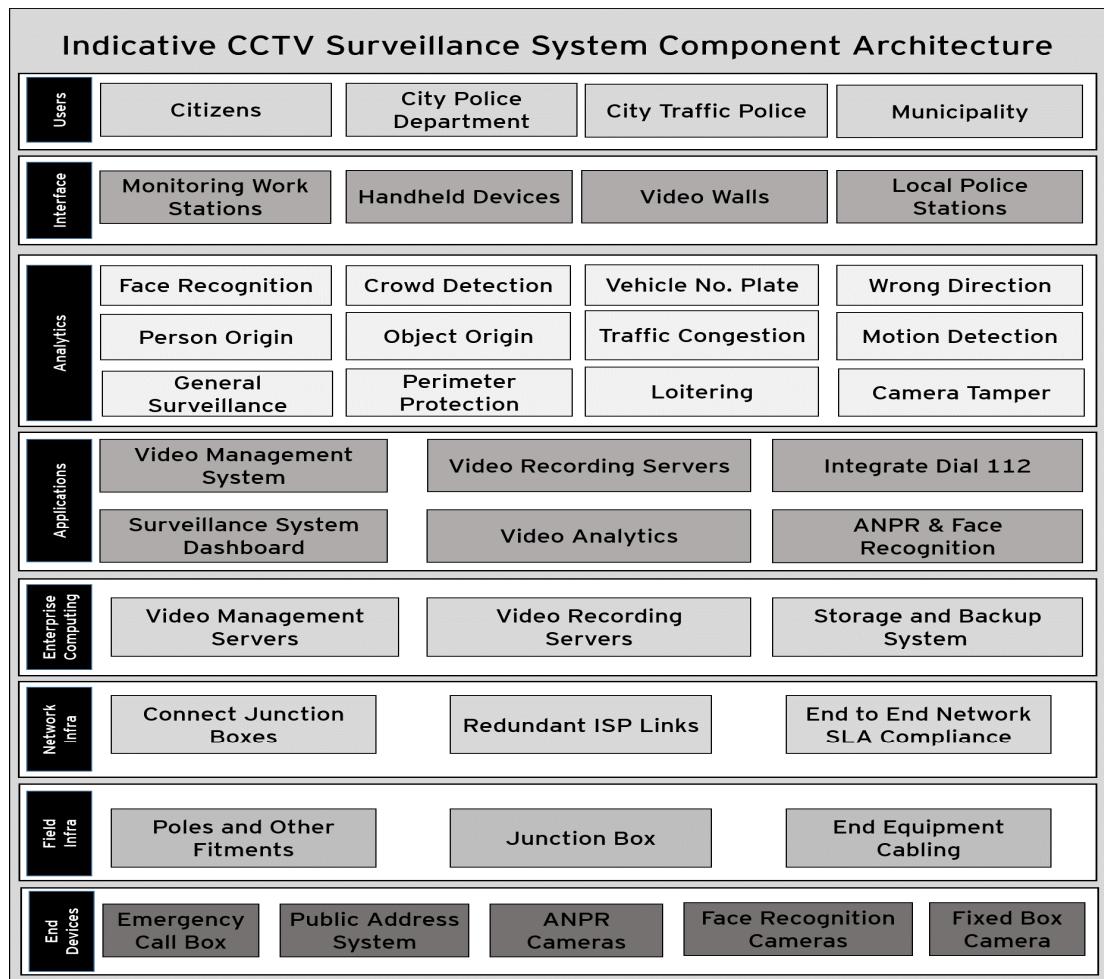
- I. Purchaser shall assist in obtaining all necessary approvals, legal permissions, No Objection Certificate (NOC) from various departments to execute the project. MSI shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. MSI shall provide & manage all necessary paper work to pursue permission from respective authorities. No commercial/legal fees shall be applicable to Purchaser for obtaining the necessary permissions. These shall be provisioned for by the MSI in their financial bid.
- II. The MSI shall provide all material required for the mounting of components such as cameras, Air Quality Monitoring Stations with local displays, Water Quality Sensors, Variable Display Board and other field equipment. All mounting devices for installation of IP cameras to enable pan and tilt capabilities shall be included in the costs of the respective component. The same is also applicable to cross-heads and cross- arms, mounting brackets, stainless steel bands, screws and other accessories.
- III. All the equipment, software and workmanship that form a part of the service are to be under warranty throughout the term of the service contract from the date of service acceptance and commencement. The warranty shall require the MSI to be responsible to bear all cost of parts, labour, field service, pick-up and delivery related to repairs, corrections during the Project Period for any or all such incidental expenses incurred during the warranty period.
- IV. MSI shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment gets damaged /stolen for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Purchaser. All such costs shall be factored in the comprehensive insurance of field equipment for the duration of the contract.
- V. During implementation, if observed that any camera / field equipment requires change in the field of view / orientation or needs servicing or cleaning, it shall be done by MSI without any extra cost.
- VI. In case of request for change in location of field equipment post installation, the same shall be borne by Purchaser at either a unit rate as per commercials or a mutually agreed cost.
- VII. MSI shall provide training and capacity building for ASCL / Municipal Staff for all software, network and hardware systems supplied and installed as part of this DPR.
- VIII. MSI shall be responsible during the integration, testing and commissioning of all the IT Infrastructure and Data Analytics systems along with all allied equipment, software, updates, patches etc.
- IX. MSI shall supply manpower as per enclosed [Annexure - V](#) for field operations, City Operation centre, monitoring and training and capacity building for the project.
- X. Master System Integrator shall provide operations and maintenance of the infrastructure for the period of 4 years after effective date of Go-Live.

Provision, Deployment and Supervision of manpower for Implementation and Maintenance of ASCL Smart Solutions

- I. The Master System Integrator shall be responsible for sourcing of the personnel and the management of all matters relating to such personnel, to carry out the responsibilities assigned to the Master System Integrator under the Contract. In particular, these include:
  - Recruitment of the personnel possessing the qualifications prescribed in the DPR;
  - Training of the personnel;
  - Payment of salaries and benefits to the personnel;
  - Meeting all statutory obligations/ payments arising out of engaging the personnel;
  - Meeting all the liabilities arising out of the acts of the personnel
- II. During the course of the Contract, if it becomes necessary to replace any of the Key Personnel (due to non-performance or any other reason whatsoever), the Master System Integrator shall forthwith with due approval from ASCL, provide as a replacement a person of equivalent or better qualifications and experience than the resource being replaced/ or proposed in the bid
- III. The team proposed in the proposal should be on the rolls of the bidder(s) at the time of submission of the proposal. For any change of the resource or any resource being proposed for operations, the bidder should have to submit the CV of the resource, at least 2 weeks in advance for ASCL to decide on the replacement.

### 3.2 City Surveillance

The MSI shall perform survey of all the existing IP Camera locations. There are 6 existing local monitoring centres connected to 40 Camera locations. The MSI shall connect these existing local monitoring centres with the proposed Integrated Command and Control Centre. Various components of the project, including users of the system are shown in the diagram below:



### 3.2.1 Installation of Standard and Cantilever GI Poles

- I. The MSI shall ensure that all pole installations are done as per satisfaction of Purchaser
- II. MSI shall meet all functional and technical requirements of Standard and Cantilever galvanized iron poles as specified in this DPR
- III. MSI shall provide structural calculations and drawings for the approval of Purchaser before commencing installation. The design shall match with common design standards as applicable under the jurisdiction of purchaser/authorized entity
- IV. MSI shall coordinate with concerned authorities/municipalities for installation
- V. Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed
- VI. MSI shall ensure that physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed
- VII. For installation of IP Cameras, PTZ Cameras, Public Address System (PAS), Variable Message Signboards (VMS) etc. MSI shall provide appropriate poles & cantilevers and any supporting structures
- VIII. The MSI shall use existing poles in Amritsar City for installing cameras where ever feasible. The quantity of poles as mentioned in DPR BOM is indicative and may vary

- after detailed site survey. Any additional required poles shall be procure by client on unit rates quoted by MSI after mutual discussion
- IX. MSI shall be required to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning
  - X. MSI shall ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically. The designs of the poles shall be approved by ASCL and AMC before installation starts and that necessary design changes incorporated after reviews
  - XI. MSI shall use the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box
  - XII. The poles shall be installed by MSI with base plate, pole door, pole distributor block and cover.
  - XIII. The poles installed by MSI shall have proper grounding, earthing and bonding as per relevant standards (to be specified by MSI) for such structures
  - XIV. Base frames and screws shall be delivered along with poles and installed by the MSI
  - XV. In case the cameras need to be installed beside or above the signal heads, suitable stainless steel extensions for poles need to be provided and installed by the MSI so that there is clear line of sight
  - XVI. MSI shall be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles/cantilevers for IP cameras , Variable Messaging Sign boards (for Air Quality Monitoring Station displays) and other equipment

### 3.2.2 Outdoor Cabinets / Junction Boxes

- I. MSI shall ensure that each location shall be fitted with outdoor cabinets sized and dimensioned to host all equipment necessary to operate Surveillance and future Traffic management and enforcement Systems as defined in this DPR. The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the intersection or nearby
- II. MSI shall ensure that all junction boxes installed at Traffic Junction, Traffic Hotspots and other important locations shall be modular and expandable to host and support equipment as part of Traffic Management and Enforcement Systems planned in next phase of Amritsar city. The battery, power supply and distribution shall be expandable to meet requirements of Traffic systems. The MSI shall reserve additional free space in the intersection controller cabinet to accommodate the future system requirements
- III. MSI shall ensure that boxes shall be dustproof and impermeable to splash-water. They shall be suitable for outdoor environmental conditions in Amritsar. They shall have separate lockable doors for:
  - a. Power cabinet: This cabinet shall house the electricity meter, rectifier, battery bank and the power supply system
  - b. Control cabinet: This cabinet shall house the electronic components required for all the field components (Surveillance Cameras, ANPR Cameras, Face

- Recognition Cameras, Public Announcement Systems, Traffic Detection and Management Systems etc.) at that particular location. The typical end equipment housed in the junction box shall include e.g. ANPR LPU, Face Recognition LPU, PA External Amplifiers, Intelligent Traffic Light Controllers, and Industrial Grade Ethernet to Fibre Optic Switches etc.
- IV. MSI shall ensure that internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power, marked with identifiers and installed in proper cable guidance trays
  - V. The cabinets shall be of robust construction and shall include 3-point security-locking mechanisms to prevent unauthorized access to the field equipment
  - VI. The MSI shall ensure that all Junction Box enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters for temperature and humidity control that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation
  - VII. MSI shall ensure that all the hardware is placed inside the junction boxes that could withstand temperatures prevalent in Amritsar City throughout the year

### 3.2.3 Civil and Electrical Works

MSI shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:

- a. Preparation of concrete foundation for Galvanized Poles & Cantilevers Poles
  - b. Laying of GI Pipes (B Class) complete with GI fitting where required
  - c. Hard soil deep digging and backfilling after cabling where required
  - d. Soft soil deep digging and backfilling after cabling where required
  - e. Chambers with metal cover at every junction box, pole and at road crossings
  - f. Concrete foundation from the Ground for outdoor racks
  - g. Any other work as required by municipal or smart city inspection teams
- I. MSI shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that MSI plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, if applicable.
  - II. MSI shall carry out all the electrical work required for powering all the components of the System.
  - III. Electrical installation and wiring shall conform to the electrical codes of India.
  - IV. MSI shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via Junction Box, housing the power supply, with minimum backup as defined in this DPR,
  - V. For the wired cameras, MSI shall provision for drawing power through PoE/POE+ (Power over Ethernet) as primary method and shall use dedicated power cable laid separately along with STP/SFTP cable only in exclusive cases, in case POE/POE+ is not possible.

- VI. Registration of electrical connections at all field sites shall be done in the name of MSI/Purchaser as agreed and finalized in the contract agreement. The cost of electricity for all field equipment and junction boxes in contract period shall be borne by the bidder.
- VII. MSI shall house the electricity meters inside the power cabinet as mentioned in the controller Cabinet section as above.

### 3.2.4 Grounding, Earthing, Bonding and Surge Protection Measures

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

### 3.2.5 IP Camera Surveillance

The MSI shall be responsible for supply, design, installation, commissioning, testing, and integration of city surveillance system along with operations and maintenance for 4 years from effective date of Go-Live. The broad scope of service shall include but not limited to the following:

- I. MSI shall meet all functional and technical requirements of IP Camera Surveillance system as specified in this DPR
- II. The MSI shall survey all the existing IP Camera locations and local monitoring stations and shall integrate the same with Integrated Command and Control Centre (ICCC)
- III. MSI shall describe in detail the design, operational and physical requirements of the proposed IP Camera Surveillance system, to demonstrate compliance with all the specified requirements in this DPR
- IV. The MSI shall install IP Camera based monitoring system at locations across Amritsar city as given in the [Annexure-II](#)
- V. MSI shall also survey the proposed locations and suggest any changes in locations mentioned in DPR based on detailed site survey and feasibility study
- VI. The MSI shall undertake stakeholder consultations and exercise due diligence for selection and placement of surveillance cameras to ensure the optimized coverage of all locations, the traffic junctions along with all associated junction arms, performance of video analytics on the field and for rugged operations

- VII. The MSI shall supply, design, install, commission, test, integrate the surveillance network on lease basis as defined in the DPR and as per technical specifications; all camera wiring connections for the system shall be installed by the MSI
- VIII. The MSI shall supply all of the necessary equipment for the camera operations including camera housings, local processing units, mountings, camera poles, switches, cabling, and shall make all network connections to the junction box
- IX. The MSI shall install all software for video analytics and process video feed as per functional requirements and technical specifications in this document
- X. Preventive maintenance shall be carried out once in a quarter along with corrective maintenance and also on demand when calls are placed by Purchaser or its designated agency.
- XI. MSI shall be responsible for operations and maintenance of all the supplied and installed equipment's during the entire O&M phase
- XII. In addition to above, the MSI shall be fully responsible for all maintenance activities for the period between installation of equipment and roll-out of the system
- XIII. The site has to be maintained by MSI against damages during the contract period
- XIV. All the camera and equipment (Damage / Repair / Theft) shall be maintained by Master System Integrator at his own cost
- XV. Periodic preventive maintenance schedules are to be established and executed as required.
- XVI. Maintenance plan and schedule have to be approved by the ASCL
- XVII. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.2.6 Automatic Number Plate Recognition

- I. MSI shall meet all functional and technical requirements of Automatic Number Plate Recognition (ANPR) system as specified in this DPR
- II. MSI shall provide ANPR solution at the identified locations including all cameras, local processing units and other accessories
- III. MSI shall describe in detail the design, operational and physical requirements of the proposed ANPR system, to demonstrate compliance with all the specified requirements in this DPR
- IV. MSI shall integrate ANPR Solution with Video Management System (VMS)
- V. The MSI shall provide enable ANPR LPU and ANPR software to process the license plate image using OCR software for getting the registration number of the vehicle with highest possible accuracy. The system shall be able to process the image of the number plate for detection of alpha numerical characters. System shall be able to identify stolen/suspected vehicles in real-time on GIS maps of Amritsar City at all locations where ANPR is installed. This shall be done by cross checking against police database/record system and verifying the vehicle characteristics with vehicle database like Vahaan
- VI. MSI shall enable ANPR cameras to provide a separate video stream to the ICCC for surveillance video recording and evidence collection purpose
- VII. MSI shall provide ANPR system that shall provide multiple pictures of vehicle and number plates when vehicle passes by at high speed, event notification and alert

- on detection of blacklisted vehicle, image captured, number detection and recognition, event reports, customized report generation etc
- VIII. MSI shall ensure the analysis of image captured shall be done in real time. Database so created from the images captured & analysis shall store the following:
- Details of vehicle like Registration No. either full or partial, Chassis No., Engine No., Body Type, Fuel Type, Colour, Name of Manufacturer, Make/Model etc.
  - Number and time of entries and exits at various facilities
  - License plate numbers
  - Validation/Analysis results etc.
- IX. MSI shall maintain complete ANPR system during the O&M period
- X. MSI shall also responsible for any damage / repair / theft of all the system installed in the end locations
- XI. MSI shall take the periodic preventive maintenance schedules are to be established and executed as required
- XII. MSI shall schedule the maintenance plan from getting the approval from ASCL
- XIII. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.3 Public Address system

- The MSI shall install Public Address System at intersections, public places, market places or those critical locations as identified by Purchaser to make important announcements for the public
- The MSI shall comply with all functional and technical requirements of the Public Address System as per DPR
- The PA system software installed by MSI at ICCC shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also be able deliver pre-recorded messages to the loud speakers attached to them over the IP network and locally attached media for public announcements
- MSI shall ensure that the system shall contain an IP based amplifier and uses PoE/POE+ power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster)
- The MSI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of DPR
- The MSI shall install IP based Public Address System as part of the information dissemination system at 25 locations in the city as mentioned in [Annexure VI](#). These systems shall be deployed at identified junction to make public interest announcements. The system deployed shall be IP based and have the capability to be managed and controlled from the ICCC room
- MSI shall maintain all the Public Address System and Panic Button during the O&M period
- MSI shall also responsible for any damage / repair / theft of all the system installed in the end locations

- IX. MSI shall take the periodic preventive maintenance schedules are to be established and executed as required
- X. MSI shall schedule the maintenance plan from getting the approval from ASCL
- XI. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

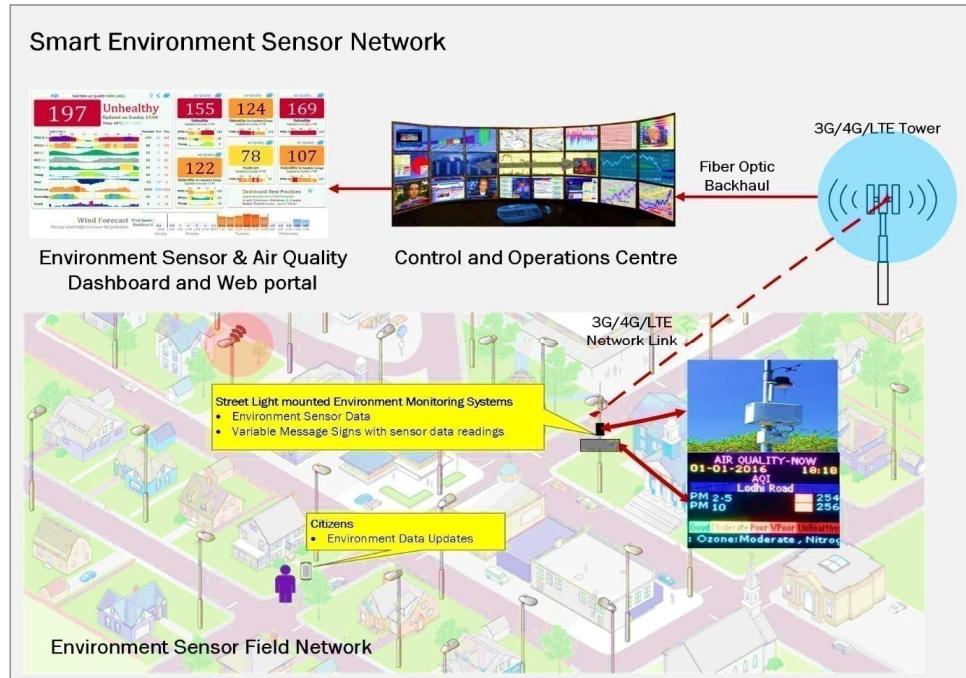
### 3.4 Emergency Call Box with Panic Button

- I. The MSI shall comply with all functional and technical requirements of the Emergency Call Box Solution with Panic Button as per DPR
- II. The MSI shall also install Emergency Call Box/Panic buttons at 10 locations in the city. These systems shall be deployed at identified locations for ease of access by citizens of Amritsar city
- III. The MSI, in consultation with police can propose alternate locations apart from the locations mentioned in this DPR for installing the ECB with panic button system where their effectiveness in helping citizens in distress conditions related to law and order incidents or traffic accidents shall be maximized
- IV. Amritsar Traffic Police shall review and approve the proposed locations. The MSI shall install the ECB system with panic buttons on the approved locations

### 3.5 Air Quality Monitoring Stations

- I. The MSI shall comply with all functional and technical requirements of the Emergency Call Box Solution with Panic Button as per DPR
- II. MSI shall install the Air Quality monitoring stations and local displays at various identified locations as per [Annexure III](#). In Amritsar three Air Quality Monitoring Stations have already implemented and are monitoring critical air quality parameters. The MSI shall install additional Air Quality Monitoring stations with sensors such as NO<sub>2</sub>, NO<sub>x</sub>, SO<sub>2</sub>, CO, O<sub>3</sub>, CO<sub>2</sub>, PM 2.5, PM 10, Temperature, Humidity etc. at 6 other identified locations
- III. MSI shall integrate the Air Quality Monitoring stations with the central control system to capture and display/ provide feed on the above mentioned air quality parameters at website / portal / mobile application
- IV. MSI shall collate the data centrally at the City Operation Centre, and analysed as per the mentioned functional requirements. The MSI shall also integrate with the existing and new sensor data with the city operation centre and centre and state pollution control boards through web, mobile and API interfaces
- V. MSI shall relay the Information instantaneously to digital signage installed alongside the Air Quality Monitoring stations which lets customers know regarding the prevalent air quality conditions
- VI. The site interiors have to be maintained against damages during the contract period
- VII. All the sensors (Damage / repair / Theft) shall be maintained by Master System Integrator
- VIII. Periodic preventive maintenance schedules are to be established and executed as required
- IX. Maintenance plan and schedule have to be approved by the ASCL
- X. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

XI. Proposed solution for Air Quality Monitoring Stations is shown in diagram below:



### 3.6 Online Waste Water Quality Monitoring System

- I. The MSI shall comply with functional and technical requirements as specified in the DPR
- II. The broad scope of work of the bidder during the contract period shall be to Design, Develop, Supply, Install, Test and Commission the Online Waste Water Quality Monitoring System along with providing Operations and Maintenance services, for a period of 3 years from effective date of Go-Live.
- III. Online Waste Water Quality Monitoring Stations shall be installed by MSI at the Tung Dhab and City Outfall Drainage Canals
- IV. MSI shall supply Online Waste Water Quality Monitoring Stations to measure pH, temperature, BOD, COD, TOC, TSS, DO, NH4-N, NO3-N, Oil and Grease using Intelligent Edge Gateways integrated with probe analysers. The OWQMS system shall be continuously monitoring the above mentioned parameters at the Tung Dhab and Cityout falls drain
- V. MSI shall be responsible for data transmission and integration of OWQMS system with the ICCC using open SCADA/IoT communication protocols
- VI. The MSI shall be responsible for securing the field infrastructure like electrical panels and floating in-situ buoys with probes using protective fencing and chains anchoring the buoys to the embankment respectively
- VII. The site has to be maintained by MSI against damages during the contract period
- VIII. All the analyser (Damage / repair / Theft) shall be maintained by System Integrator
- IX. Periodic preventive maintenance schedules are to be done on quarterly basis or on demand in case of client request and executed as required during the contract period
- X. Maintenance plan and schedule have to be approved by the ASCL
- XI. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance with any downtime.

### 3.7 Communication Network

#### 3.7.1 General Guidelines

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

Critical network design parameters such as security, reliability, scalability, manageability, interoperability and resiliency in end-to-end service oriented network delivery shall be considered when taking network backbone on lease across the city from existing service providers.

Free Right of Way shall be provided by AMC for any new network laying that is to be laid as part of smart city initiative and for sole usage of smart city applications. ASCL shall help in providing ROW permissions by coordinating with AMC.

The network backbone is expected to provide a converged network, bringing together different city management vertical solutions on a common network infrastructure for Amritsar. The converged network shall facilitate information exchange between resources and applications across different domains.

The network architecture being proposed shall comply with the SLA's, best practices and industry standards to ensure high availability, scalability, manageability and security for the information, services and solutions being managed on the network.

The designed network shall provide uninterrupted services across the Amritsar City connecting seamlessly with various stakeholders. With the capability to handle high bandwidth applications with low network latency.

The various locations that need to be connected on network are mentioned but not limited to, Zonal offices, AMC Head Office, Integrated Command and Control Centre (ICCC), Ward offices, Hospitals and other City Administration's important buildings, Field locations which have IoT / Smart City devices.

The Master System Integrator (MSI) shall adhere to the below guidelines while executing the work:

- I. The MSI shall submit the work plan and implementation schedule with list of supplied equipment and personnel to be deployed on field for execution of works for approval of Client.
- II. The MSI shall commence work post approval of work plan and schedule by the Client.
- III. The MSI shall inform all concerned authorities and obtain NOC or permissions as required before starting the work.
- IV. The MSI shall register and get approval from concerned Government authorities to carry out the work as required.
- V. The MSI shall adhere to guidelines issued by concerned Government authorities while executing the work.
- VI. The skilled manpower, testing instruments and equipment & material required for proper maintenance and meeting the SLA obligation shall be the sole responsibility of the successful MSI.

- VII. The MSI should have proper legal agreement with the OEM to guarantee quality, timely supply, performance, warranty and O&M during the full life-cycle of the contract.
- VIII. The MSI shall carry out periodical maintenance of the network commissioned and shall submit the report on quarterly basis during the O&M phase.
- IX. MSI shall responsible in case of theft or physically damage the equipment and FIR shall be lodges by the MSI in such cases. In such cases, MSI will pay for both, material as well as service charges and shall be completely responsible for security of field equipment.
- X. The cost of pre-notified planned shifting of cable route due to other reasons like widening of road, construction of bridges or asked by central / state authorities (PWD/NHAI/Railway etc.) or force majeure reasons will be paid by ASCL. The same condition will be applicable during O&M period.

### 3.7.2 Leasing of Network

- I. The MSI shall provide the network with sufficient capacity available on Lease to ASCL for entire project duration
- II. The MSI can provide existing network or can take network from other service providers on lease
- III. The MSI shall provide network connectivity at all required locations as mentioned in the document. No location shall be left un-covered irrespective of existing network is available or new network has to be laid
- IV. If UG network is not available in any area and permission to lay New UG network is difficult due to feasibility or other issues, MSI can lay OH network in that area with written permission of ASCL and AMC
- V. The MSI shall provide end to end connectivity from all locations to Central Location in Data Centre through various technologies mentioned here but not limited to Point to Point / SD-WAN / MPLS-VPN / Radio connectivity etc. over fibre or copper physical media while meeting all SLA's defined in this document
- VI. The MSI shall be responsible to provide all Active / Passive equipment's from Central Location to Last point of connectivity
- VII. The MSI shall upgrade the equipment's free of cost, if required in future, to ensure that services run smoothly and SLA is not breached
- VIII. The MSI shall be responsible to provide any Monitoring / Managing Software which shall be required to monitor/ manage the Leased network
- IX. All the Locations must be connected in Ring till the last point of connectivity from two different sides
- X. The Leased network shall be future scalable and support upgrade in terms of network, bandwidth and field components etc.
- XI. The MSI shall be responsible for O&M of leased network for the said period from the date of lease of network
- XII. Any addition in the number of locations shall need to be connected as per the agreed terms and conditions for already connected sites. Same terms and conditions shall be applicable for change or removal of any site from earlier selected sites

- XIII. Routine inspection, viz, patrolling on the routes, to identify area where Cable is exposed and prone to cut due to natural wear and tear etc.
- XIV. Fault rectification of cable cuts along routes
- XV. Replacement of cable routes due to non-viability of transmission link
- XVI. Ensure availability of cable route marker along the route at regular intervals
- XVII. Maintain proper condition of joint boxes
- XVIII. Prevent third party damages viz, theft, damage by other U/G utility etc.
- XIX. Maintain condition of cable with casing or with special arrangements near critical areas viz, major bridges, railway crossing, pipe line crossing etc.
- XX. Visual inspection of joint boxes and junction boxes to check ingress of water, foreign particles etc.
- XXI. Preventive and regular checks of power plant battery, generator, ac & remote alarm units
- XXII. Periodic measurement of the link attenuation loss to ensure that the link is free from any point loss defects etc.
- XXIII. Maintaining history of events, analysis and reporting, public liaisoning with concerned authorities

### 3.7.3 Fault Restoration Services

- I. The MSI shall deploy Maintenance Teams at the designated locations to ensure SLA adherence. The Maintenance teams shall comprise of manpower, logistics, required tools/tackles/machinery & equipment etc.
- II. The MSI shall provide maintenance service on round the clock basis for attending & rectifying the network faults in minimum downtime (including travel time) from the time of lodging the complaint to the representative of lead MSI at their designated office. The Lead MSI shall provide all assistance including providing manpower, transportation of men and materials etc. if required in the event of link failure due to any other reason
- III. The Lead MSI shall provide conveyance facilities for maintenance, for transporting the manpower, tools/tackles, test/ measuring equipment and consumables. Suitable vehicle shall be available round the clock with each of the maintenance team. Vehicle should be in good working condition and shall not be more than five years old
- IV. The MSI shall provide communication facilities to the maintenance teams. This shall include landline phone at office location and mobile phone to members of the maintenance teams for the purpose of contacting on an urgent need basis. The team-in-charge should have mobile phone of mobile operator whose coverage is available in the desired section and it should be always on
- V. The MSI shall be required to carry out maintenance activities which include identification of fault/cut on ground, obtaining permission from local authorities if required, excavation of earth to expose cable, laying of required length of cable with protection wherever required, installation of Jointing pit & back filling of pit with sand, supply and installation of cable Route Markers and Joint Markers as per specifications

- VI. The MSI shall arrange for logistics to provide facilities such as AC/DC power source, lighting arrangement, dewatering facility, DG sets etc., which may be required during the execution of maintenance job at site
- VII. Optimum functionality of maintenance teams is a prime necessity to carry out day to day maintenance of network links. Cable and accessories spares to cater for repair of at least 10 cable cuts shall be maintained with each of these teams at all times
- VIII. MSI shall take insurance for all the workmen engaged under this contract and as per labour laws applicable from time to time
- IX. After attending the fault & permanent restoration a Fault-Rectification report, jointly signed by ASCL & MSI, shall be generated for the closure of the complaint
- X. Any other job required for the restoration of the cable cut in totality is to be taken up by the MSI. In case, the site condition is not favourable for the immediate restoration of the fault, the temporary restoration of the in-service cable shall be taken up immediately with the approval of authorized representative of ASCL. Permanent restoration work shall not be considered in breakdown time unless there is again link break during restoration job. Permanent restoration of joint pits is to be carried out by MSI within reasonable time of fault / cable cut. In case the site is not conducive for permanent restoration, some arrangement of manpower has to be done by MSI for safeguarding exposed cable till permanent restoration. No extra payment shall be given to MSI on account of deployment of additional manpower. In such case, further cut in that stretch shall not be counted in SLA measurements as this is non attributable to PIA
- XI. In case of any breakdown in the network, MSI shall be responsible for obtaining approval from concerned authorities as required for carrying out the repair. ASCL can assist in getting permission for repair in few cases where there is urgency
- XII. Drains, pipes, cables and similar services encountered in the course of the works shall be guarded by the MSI at his own cost, so that they may continue in full and uninterrupted use to the satisfaction of the owners thereof
- XIII. Should any damage be done by the MSI to any AC power mains, utility pipelines cables or lines (whether above or below ground etc.) whether or not shown on the drawings, the MSI must make good or bear the cost of making good the same without delay to the satisfaction of the Engineer-in-Charge
- XIV. MSI shall observe all national and local laws, ordinances, rules and regulations and requirements pertaining to the work and shall be responsible for extra costs arising from violations of the same
- XV. MSI shall have at all times during the performance of the work, a competent supervisor. Any instructions given to such supervisor shall be considered as having been given to the MSI
- XVI. The MSI shall employ as many personnel as required to comply with the local rules and administrative orders governing the Working Hours of Employment. The MSI shall be responsible for compliance with all statutory requirements including personnel related matters
- XVII. The minimum down time shall include time taken in restoration of fault/ cut caused by any means like miscreant activity at day or night, due to work done by any other

- organization, due to development of high losses/ break at existing joints, fault caused due to rodent, ant etc.
- XVIII. In case of partial damage of the cable or development of high loss in the working and spare cable cut at any time (day/night) by miscreants or by any agency, the responsibility of repairing the defective cable lies with the MSI
- XIX. In case, MSI fails to completely restore (as per original condition) or submit test reports (power level in live equipment) to establish completion of work, a penalty shall be levied for the work involved at site

#### 3.7.4 Examination of Finished Work

- I. When finished work is taken down for the purpose of inspection for any reason, the MSI shall bear the entire expenses incidental thereto in the event that the said work is found to be defective. This situation may be applicable to both planned work as also to emergency restoration.
- II. During the maintenance or fault rectification work, should any damage occur to the other cables, MSI is liable to pay compensation as demanded by the respective owner.

#### 3.7.5 System Security Safeguards and Risk Mitigation Strategy

The following threats from Intentional Attacks should be addressed by Master System Integrator:

- I. Eavesdropping/wiretapping may affect availability, integrity and confidentiality of data and information systems respectively.
- II. Theft of information/data or technology that may affect availability and confidentiality.
- III. Tampering/alteration of information/data, applications or technology via several means e.g. information leak, reply attacks, malware etc. has effect on availability, integrity and non-repudiation/accountability.
- IV. Unauthorized use/access of information/data, applications or technology in an unauthorized way which includes any unauthorized connection to a network, data leaks, and browsing files, acquiring private data, controlling field components and using resources for personal use.
- V. 24x7 monitoring & management of availability & security of the infrastructure and assets
- VI. Ensure overall security – ensure installation and management of every security component at every layer including physical security
- VII. Reporting security incidents and resolution of the same
- VIII. Reporting security incidents and co-ordinate resolution
- IX. Providing root cause analysis for all defined problems

#### 3.7.6 Commissioning of Active / Passive Equipment's and Infrastructure

- I. Procure & Supply all the active / passive components and accessories required for smart city solutions as mentioned in the indicative bill of material.
- II. Install and Commission procured material at respective sites.

- III. Provide comprehensive onsite OEM warranty for all the supplied products/ services at all the designated project locations for the entire project period.

### 3.7.7 Training and Capacity Building

- I. MSI shall prepare and submit detailed User manuals to ASCL for review and approval.
- II. User Manuals are expected to be prepared in bilingual (English & Punjabi).
- III. MSI shall impart operational and technical training to internal users on the infrastructure that is being used, its physical properties, usages and mechanism.
- IV. MSI shall update training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.

## 3.8 Integrated Command Control Centre

The Integrated Command Control Centre (ICCC) will house City Operations Centre (COC) for City Municipal Corporation functions and Command & Control Centre (CCC) for Police functions. The ICCC shall be used by agencies to monitor their respective functions and responsibilities.

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

In this DPR it is envisaged to have ICCC for police department and city operations. The scope of work of MSI for the ICCC shall include:

- I. The MSI shall design, supply, install, implement, configure, and test the component sub-systems of the ICCC followed by operations and management as per the contract for the Municipal functions and Police department for period of 4 years from Effective Date of Go-Live.
- II. The MSI shall coordinate with various agencies in an integrated manner
- III. The MSI shall analyse and present the data as per the requirements of the ASCL.
- IV. The MSI shall deploy necessary analytics and visualisation tools as per the requirements of the ASCL.
- V. MSI shall operate and manage the ICCC 24X7.
- VI. The MSI shall deliver a roll out strategy for implementing and integrating the smart solutions of the city utilities and surveillance in the ICCC.
- VII. The MSI shall implement, monitor the SLA for the assets in the ICCC.
- VIII. The MSI shall manage the operations and ensure to maintain the ICCC as per the Industry standards and Continuous process improvement shall be ensured by the MSI for better performance.
- IX. MSI shall implement, monitor and manage the security policies and procedures for the IT and NON IT assets as per the leading industry practices.

- X. MSI shall prepare SOP for the Municipal function control centre and the surveillance control centre.
- XI. MSI shall co-ordinate with various agencies for successful implementation, operations and maintenance of the project
- XII. MSI shall ensure inter-operability, seamless integration and data sharing of data between various solutions by building required APIs between end solutions and ICCC Software Platform. These shall include all sub-systems in this DPR and future solutions rolled out by the smart city during contract period of the MSI.
- XIII. MSI shall ensure to abide industry- standard data transports and open protocols.
- XIV. MSI shall share report of various data using reporting tools and visualisation tools as per the requirements of ASCL.
- XV. MSI shall deploy prescriptive and predictive analytics where ever applicable as per the requirements of ASCL.
- XVI. MSI shall ensure High level of perimeter and internal IT security at the ICCC and shall be responsible for rectifying all security incidents as per SLA requirements.
- XVII. MSI shall supply the necessary communication equipment, IP telephony and other necessary infrastructure for the municipal and police department staff to be deployed in the ICCC.
- XVIII. The MSI shall ensure that the overall work shall be in reference to standards published as per ISO 37120 and World Council of City Data (WCCD).

### 3.8.1 Setting up ICCC (Integrated Command Control Centre)

#### 3.8.1.1 Survey and Site Preparation

The MSI shall survey the identified site at Amritsar Municipal Corporation office 2nd Floor, and submit necessary layouts for approval: civil, electrical, power and cooling. For ICCC and Data Centre, space has been ear marked for the same.

- I. The MSI shall prepare necessary layouts, architectural, civil, electrical, interior drawings and submit the same for ASCL approval.
- II. Upon approval, MSI shall complete the necessary civil, electrical, cooling and interior work. The MSI shall also be responsible for the upkeep, operations and maintenance of the ICCC infrastructure during the contract period at his own cost.
- III. The MSI shall be responsible for the final design, sizing, procurement, deployment, commissioning, and integration and testing of the security systems at the ICCC.

#### 3.8.1.2 Delivery

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

#### 3.8.1.3 Installation and Commissioning

The Master System Integrator is responsible for all unpacking, assembling, wiring, installations, cabling, interconnection and commissioning of the delivered components and

its required integration. The installation and testing includes all the networking devices but not limited to the following.

- I. Installation of all items as per BoQ
- II. Installation and commissioning of line items as per BoQ
- III. Carrying out necessary civil, electrical work, cooling, power as per BoQ
- IV. Upon completion of the installation, Installation certification has to be submitted to the ASCL.
- V. Completion of installation does not mean the effective date of Go-Live date of the project. The AMC and warranty of the product shall start from the effective date of Go-Live of the project.
- VI. Commissioning has to be carried out as per the project requirements.
- VII. The installation document should contain Physical layouts, Electrical layouts, Civil Architectures, LAN Drawings. Revised document has to be submitted to ASCL, whenever there are any changes during the period of the contract.

#### 3.8.1.4 Acceptance Testing

- I. Acceptance team/committee have to be constituted by the MSI
- II. Detailed acceptance test procedures and test plans have to be submitted to ASCL office for vetting before the start of commissioning of equipment. Acceptance test plan describing the detailed schedule of primary and sub tasks has to be submitted to ASCL. Acceptance test procedure as per the industry standards has to be submitted to ASCL. Acceptance tests have to be carried out as per the accepted procedure and report has to be submitted for ASCL approval.
- III. Upon acceptance of the test procedures, acceptance testing has to be carried out by the MSI as per the approved acceptance test procedure.
- IV. Upon completion of the testing, trial run has to be completed for a defined period.
- V. Based on the testing, necessary recommendations of the committee has to be implemented before the commencement of the trial run period.
- VI. Multiple trial runs shall be required if ASCL to provide proof of operations and compliance to SLA's and performance criteria
- VII. Detailed acceptance reports have to be submitted to ASCL office.
- VIII. The testing shall be performed after the completion of installation at the site.
- IX. Necessary test and measurement equipment's/special tools for installation, testing and commissioning of the new components, for the purpose of initiating the operation & maintenance phase of new hardware should be made available by the Master System Integrator. Necessary calibration should have been done and the certification of the same should be made available if requested by ASCL.
- X. The designated individuals/Team by ASCL shall verify the component level details during this testing and shall sign the installation report after successful completion of the post installation testing activities. Defects / shortcomings brought out in this testing shall have to be attended as per the contract within the permitted time schedule.

### 3.8.1.5 Manuals

The Master System Integrator shall provide complete technical documentation of hardware, firmware, all subsystems, operating systems, compiler, system software and the other software. The source code shall also be shared with ASCL. The manuals, wherever applicable shall be in English. All the applicable manuals/documents/Data Sheets for the items delivered and installed should be submitted. Unless and otherwise agreed, the equipment delivered and services rendered shall not be considered as completed for the purpose of Effective Date of Go-Live until such manuals and drawings have been supplied to the ASCL.

Before the commencement of trial run, the Master System Integrator shall supply all the operation and maintenance procedures, (together with drawings of the goods and services where applicable).

### 3.8.1.6 Product License

All products license and warranty are to be procured in the name of ASCL. Copy of the license terms and conditions has to be submitted to ASCL during trial run.

### 3.8.1.7 Facility Management Services

The Master System Integrator shall carry out the Facility Management Services on a 24x7 basis towards Electrical systems, DG, UPS, HVAC & Control systems to meet the SLA, specifications of each component. An Operation & Maintenance manual should be taken as reference for facility management services but ASCL reserves the right to amend the manual as per requirement during the course of the operations.

Operations and Management Manuals as per ISO 20000 standards have to be submitted to the ASCL before the commencement of the trial run. The trial run has to be carried out as per the approved operations and management manual.

ICCC (COC & CCC), Server farm Area, NOC- The entire infrastructure management would be managed in multiple shifts covering the all 7 days a week.

The scope of the FMS services must include as mentioned below but may not be restricted to

- I. The site interiors have to be maintained against damages during the contract period
- II. The House keeping management for basic facilities such as drinking water shall be managed by the Master System Integrator.
- III. Periodic preventive maintenance schedules are to be established and executed as required
- IV. Maintenance plan and schedule have to be approved by the ASCL.
- V. 7 days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.8 Electrical System

- I. All electrical System at Project site has to be maintained by licensed electricians (C/B) who would be responsible for electrical upkeep.

- II. Electricity charges of project site shall be paid by Master System Integrator and shall be reimbursed by ASCL.
- III. Periodic preventive maintenance schedules are to be established and executed
- IV. A comprehensive FMS report for the maintenance of all the electrical system on a periodical basis is to be submitted to ASCL and will be validated by ASCL along with the ASCLs authorised agency.
- V. All the corrective actions have to be completed as directed by ASCL
- VI. Maintenance plan and schedule have to be approved by the ASCL.
- VII. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.9 Diesel Generator

- I. Master System Integrator shall be responsible for consumables such as diesel, engine oil, air & oil filters.
- II. DG back up has to be made available 24/7 and necessary fuel stock and back up arrangement has to be made in place.
- III. A detailed logbook is to be maintained for diesel consumption.
- IV. The diesel purchase invoice has to be maintained for all diesel purchases and shall be reimbursed by ASCL
- V. Preventive maintenance schedules are to be established and executed. Periodic maintenance reports are to be submitted to ASCL and will be reviewed by ASCL or Authorised Representative.
- VI. Defects or malfunctions if identified are to be fixed with immediate corrective action and may include replacement of spare parts, corrective action on existing equipment or requesting a service call from the OEM to run diagnostic tests.
- VII. Maintenance plan and schedule have to be approved by the ASCL.
- VIII. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.10 UPS

- I. Preventive maintenance schedules are to be established for UPS devices used for IT Load as well as the Auxiliary UPS systems used for emergency lighting & BMS
- II. Periodic maintenance reports are to be submitted to ASCL for review and approval
- III. Maintenance plan and schedule have to be approved by the ASCL.
- IV. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.11 Cooling Systems or HVAC

- I. Spares consumables for PAC, Comfort AC, Split AC shall be taken care by the Master System Integrator
- II. Preventive maintenance schedules are to be established and executed periodically for the PAC, CFM solutions and other cooling systems deployed at the site.
- III. MSI shall submit periodic maintenance reports to ASCL which shall be reviewed by ASCL. Defects or malfunctions identified are to be fixed with immediate corrective action and may include replacement of spare parts, corrective action on existing
- IV. All corrective actions have to be taken as directed by ASCL

- V. Operational cycles should be established for cooling equipment to ensure the usage of all redundant devices at optimum durations. To ensure operational readiness of any device in the event of failure of one or more devices
- VI. The following temperature has to be maintained
  - a. Server Farm Area - 21 C
  - b. Auxiliary Area - 26 C
- VII. The following humidity has to be maintained
  - a. Server Farm area: 40-60%
  - b. Auxiliary Area: 20-80%
- VIII. Maintenance plan and schedule have to be approved by the ASCL.
- IX. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.12 Integrated Building Management System

- I. All the physical & support infrastructure (such as DG set, PAC, UPS, control systems, etc.) in the Amritsar Smart City project shall be monitored on a 24x7 basis.
- II. Preventive maintenance schedules are to be established for Access Card, Fire Alarm, IP Cameras, Rodent Repellent, Water Leakage Detection system, VESDA, PA systems and must include inspection of the controllers installed in each device
- III. IP camera video recordings are to be periodically backed up by the Master System Integrator.
- IV. Any device level replacement or upgrade is to be brought to the notice of the ASCL with suitable justification for the same.
- V. Periodic maintenance reports are to be submitted to ASCL for review and approval
- VI. Maintenance plan and schedule have to be approved by the ASCL.
- VII. Seven (7) days' notice has to be submitted to ASCL office for planned maintenance

### 3.8.1.13 Other Infrastructure Management services

- I. Visitor access register has to be maintained. Prior written approval is required for entry of any visitors into the ICCC/Project site.
- II. Movement Register has to be maintained. 365X24X7 access log for a complete record of any person moving in and out of the project site.
- III. Maintenance of existing Access card level security for various parts of the ICCC, server area and other area for various members should be suitably managed by the Master System Integrator.
- IV. Access to the farm area is to be highly restricted and only selected technical personnel are to be allowed. Biometric access has to be maintained for the farm area.
- V. A separate visitor's log book is to be maintained for the farm area/Telecom Room where occasional visitors will be requested to sign in.
- VI. The Master System Integrator is expected to adhere environmental, health, security and safety practices. ASCL shall be not be responsible to the implications of any unhealthy practice or damage caused by the Master System Integrator

### 3.8.1.14 Other Infrastructure or Services

- I. The ICCC and data centre interiors to be maintained against damages during the contract period. The House keeping management for basic facilities such as drinking water, waste disposal, cleaning etc. shall be managed by the Master System Integrator.
- II. Water dispenser and regular supply of the water within the ICCC & DC should be provided by Master System Integrator
- III. Periodic preventive maintenance schedules are to be established and executed as necessary
- IV. A comprehensive Facilities maintenance services report for the status of civil & interior works is to be submitted on a periodical basis which will be certified by ASCL in coordination with the consultants as necessary and indicate if necessary repair works if any are to be carried out. All repair works to be completed as directed by ASCL
- V. All Furniture's which are not limited chairs, tables, walls plastering, paintings, floorings, glass panels, wall or glass partitions, false ceiling, lights, switches, should be kept intact as in good working conditions. Any damages to be rectified/replaced at the cost of the Master System Integrator

### 3.8.1.15 Warranty and AMC

The warranty period shall be as stated in bid document. The Master System Integrator shall, in addition, comply with the performance guarantees specified under the contract. If, for reasons attributable to the Master System Integrator these guarantees are not attained in whole or in part, the MSI shall, make changes, modifications, and/or additions to the equipment or any part thereof as may be necessary in order to attain the contractual guarantees specified in the contract at its own cost and expenses and to carry out further performance tests.

AMC/Warranty should commence from the effective date of Go-Live. The System Integrator shall submit Warranty/AMC valid for the duration of the project for all supplied hardware, software, licenses and Non IT with no extra cost in commercial part of bid. The installation will be deemed incomplete if any component of the equipment or any documentation/media is not submitted to ASCL. The Master System Integrator shall be responsible for the up keep and maintenance of the infrastructure and necessary deliverables under the scope of work during the entire warranty period.

### 3.8.1.16 Transportation

Transport of the goods to the project site(s) shall be arranged by the Master System Integrator at their cost and own risk

### 3.8.1.17 Go Live of the project

On successful acceptance of the trial run and based on test reports, the go live date shall be decided by ASCL. Effective date of Go-Live shall be considered as the warranty date for all the equipment and devices.

### 3.9 City Operation Centre (COC) for Municipal Functions at ICCC

- I. MSI shall develop, deploy, install and maintain the ICCC Software platform application that integrates various municipal smart city applications.
- II. Smart city applications in this phase shall include
  - a. Fleet Monitoring System
  - b. Online Air Quality Monitoring Systems
  - c. Online Waste Water Quality Monitoring System
  - d. IP Camera Surveillance System
  - e. Public Announcement Systems
  - f. Emergency Call Box
- III. Smart city application to be integrated by MSI in ICCC for forthcoming phases shall include;
  - a. Solid waste management system
  - b. SCADA of water, gas and electricity utility networks
  - c. Smart Parking
  - d. Intelligent Street Lighting
  - e. Variable Message Signboards
  - f. Public Wi-Fi System
  - g. Intelligent Traffic Management System
  - h. Solar Grids
  - i. E-Governance and ERP System
  - j. Geographical Information System
  - k. Citizen Engagement Platform and Mobile apps
  - l. Other applications as identified by ASCL and AMC
- IV. MSI shall ensure complete data integration along with control, monitoring and provisioning of IoT sensors and end equipment is possible from ICCC Software platform.
- V. Staff of various departments deployed in the ICCC are able to perform action as per the agreed SOP.
- VI. MSI shall ensure the transfer of feeds to other control centres and mobile phone of staff as per the application requirements.

### 3.10 Control and Command Centre (CCC) for Police Functions at ICCC

- I. MSI shall develop, deploy, install and maintain the ICCC Software platform application that integrates various police functions.
- II. MSI shall ensure that all the cameras feed are made available and controlled in the ICCC
- III. MIS shall provide video analytics dashboards for Face Recognition, ANPR and other cameras feed.
- IV. MSI shall ensure automatic object recognition and tracking using cameras feed.
- V. Control Public Address System from ICCC
- VI. MSI shall ensure two way communication through Emergency Call Box and Panic Button.

### 3.11 Integration of ICCC with Dial 112 project

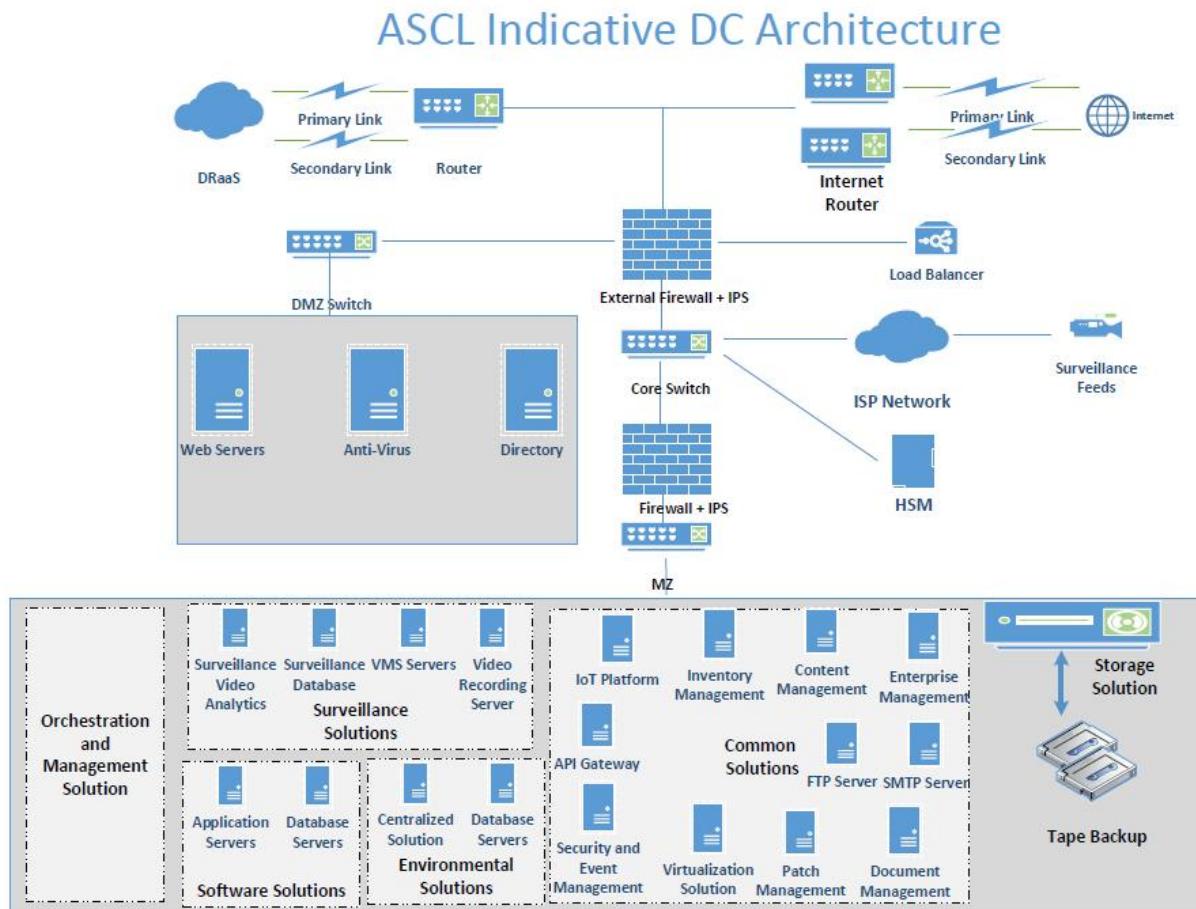
The control rooms of Police, Ambulance and fire department are planned to be integrated under single system call Dial 112. The dial 112 will be the universal number for all the emergency services. In Punjab, the Dial 112 is planned to be implemented in distributed model. In this model, there will be a centralised call taker centre and 12 dispatch centres across 12 districts. The police patrol vehicles, ambulance and fire vehicles can be dispatched from these dispatch centres.

The envisaged ICCC under smart city shall have the facility of the dispatch centre. The following are the envisaged activities

- I. MSI shall be responsible to integrate centralised call taker centre and vehicle dispatch centre with ICCC
- II. MSI shall be able to create incidents in the Dial 112 web based portal based on the alerts generated in the surveillance system
- III. MSI should be able to dispatch/communicate with the required police, fire and ambulance vehicle covered in the dial 112 system.
- IV. MSI shall be able to update the created incidents, update incidents and close the incidents based on the alerts generated by the surveillance system.
- V. MSI shall able to make out bound calls to the dispatch vehicles
- VI. MSI shall develop APIs of the Surveillance system which should be seamlessly integrated with the dial 112 for generation of the incidents.
- VII. MSI shall install three monitors in the every workstations at police command centre and city operation centre. One monitor should display the online GIS maps with cameras and their locations.
- VIII. MSI shall be responsible to generate display whenever there is an incident and the respective camera video should be played in the screen.
- IX. MSI shall integrate with dial 112 application which shall be operated from the ICCC centre.

## 3.12 Data Centre

### 3.12.1 Overall DC Architecture



Following are the outlines of the broad areas of Scope of Work for system integrator which have been further detailed in later sections:

- I. Application Design, Development, Procurement, Supply, Delivery, Installation, Configuration, Implementation, Testing, Commissioning, Operations & Maintenance
- II. Provisioning of Hosting/ Co-location Facilities for DC and maintaining readiness for future DRC
- III. Procurement and Installation of IT Infrastructure at DC and across all the smart solutions
- IV. Operations & Maintenance of all Smart Solutions
- V. Operations & Maintenance of IT Infrastructure at DC and for all the field infrastructure across all smart solutions
- VI. Security of Information and Data at DC
- VII. Provision, deployment and supervision of manpower for Implementation and Operations & Maintenance of Amritsar Smart City Solutions
- VIII. Requirement for Adherence to Standards
- IX. Acceptance Testing

The following sections details out the Scope of Work to be performed by Master System Integrator. The Master System Integrator shall be responsible for all the services, functions/ requirements listed in the following paragraph and as defined in the DPR

### 3.12.2 ASCL Data Centre

- I. The selected bidder shall provide system integration services to procure and commission the required software and infrastructure at the Data Centre.
- II. MSI shall deploy, install, configure and customize Software solutions, as mentioned in the relevant sections of this DPR and integrate with the external Agencies as provided in the functional scope.
- III. The MSI shall be completely responsible for the sourcing, installation, commissioning, testing and certification of the necessary software licenses and infrastructure required to deploy the Solution at the Data Centre in Amritsar City.
- IV. MSI shall ensure that support and maintenance, performance and up-time levels are compliant with SLAs as provide in the relevant sections of this DPR.
- V. To ensure redundancy requirements are met, MSI shall ensure that infrastructure procured by the MSI has redundancy built in.
- VI. MSI shall also provide descriptive 'Deployment Model, Diagrams and Details' so that redundancy requirements for the common Data Centre infrastructure can be addressed.
- VII. The MSI shall be responsible for sizing the hardware to support the scalability and performance requirements of the solution.
- VIII. The MSI shall ensure that the servers and storage are sized adequately and redundancy is built into the architecture that is required meet the service levels mentioned in the DPR.
- IX. The MSI shall be responsible for the sizing of necessary hardware and determining the specifications of the same in order to meet the requirements of the project
- X. MSI will be single point of contact and in the backend MSI shall ensure uptime, SLA as mentioned in SLA section of this document. Also, MSI would be responsible for procurement and deployment of the required servers at the DC site
- XI. Overall monitoring and management of the ASCL Smart Solutions implemented for the Project shall be the responsibility of Master System Integrator
- XII. Ensuring compliance to the uptime and performance requirements for solution performance
- XIII. 24x7 monitoring & management of availability & IT security of the infrastructure & assets (including data, servers, systems etc.) through the Enterprise Management Solution implemented for Project shall be the responsibility of Master System Integrator
- XIV. Implementation of a comprehensive security policy to comply with the requirements of the DPR and conforming to relevant standards (ISO 27001)
- XV. Ensuring uptime, performance and other key performance requirements of the Project including data backup & business continuity
- XVI. Perform patch management, testing and installation of software upgrades issued by the OEM/ vendors from time to time. These patches/ upgrades, before being applied on the live infrastructure of the Data Repository at DC, shall be adequately tested. Any downtime caused due to up gradation & patches shall be to the account

- of the Master System Integrator and it shall not be considered as 'Agreed Service Downtime'.
- XVII. Develop the Standard Operating Procedures (SOPs), in accordance with the ISO 27001 & ITIL standards, for Project Infrastructure management. These SOPs shall cover all the aspects including Infrastructure installation, monitoring, management, data backup & restoration, security policy, business continuity & disaster recovery, operational procedures etc. The Master System Integrator shall obtain sign-offs on the SOPs from the ASCL and shall make necessary changes, on a half yearly basis, to the fullest satisfaction of ASCL.
- XVIII. Preventive maintenance, carrying out the necessary repairs and replacement of parts wherever needed to keep the performance levels of the hardware and equipment in tune with the requirements of the SLA. Such preventive maintenance shall not be attended during working hours of the ASCL, unless inevitable and approved by the ASCL.
- XIX. Reactive maintenance that is intended to troubleshoot the system with sufficient teams
- XX. Performance tuning of system as may be needed to comply with SLA on continuous basis
- XXI. Monitor and record, server & database performance and take corrective actions to ensure performance optimization on a daily basis
- XXII. Escalation and co-ordination with other vendors/ OEMS for problem resolution wherever required
- XXIII. System administration tasks such as managing the access control system, creating and managing users, taking backups etc.
- XXIV. Ensure that daily back-up copies of the data are created and maintained safely
- XXV. Produce and maintain system audit logs on the system for a period agreed to with the ASCL. On expiry of the said period the audit logs should be archived and stored off-site.
- XXVI. Regularly review the audit logs for relevant security lapses
- XXVII. Review security advisories (such as bulletins generally available in the industry) on a regular basis to determine vulnerabilities relevant to the information assets and take necessary preventive steps
- XXVIII. Master System Integrator shall ensure helpdesk facility shall have following:
- Call logging mechanism through Phone
  - Call logging mechanism through e-mail
  - Call logging mechanism through portal
- XXIX. Helpdesk shall provide its services on all working days of ASCL between 09:00 Hrs. to 21:00 Hrs.
- XXX. All complaints/ grievances made by any mode shall be recorded and the records maintained for reference for a period of at least 3 months from the date of resolution of the problem
- XXXI. The Master System Integrator shall provide the following helpdesk performance monitoring reports:
- Calls per week, month or other period
  - Numeric and graphical representation of call volume
  - Calls tracked by type

d. Number of dropped calls

XXXII. The Master System Integrator shall provide at least six member team for the helpdesk

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

### 3.12.3 Site Preparation

- I. The MSI shall be required to undertake detailed assessment of the requirements Data centre and commission required IT and non-IT infrastructure and also carry out the civil/ electrical work as required.
- II. Department shall carry out a detail assessment of the proposed design solution and review design for DC including all its components such as Server Room, operators seating arrangement, office space, supervisors seating arrangement, visitors' gallery, reception area etc. on the parameters of overall Design, Safety & Security and aesthetics and reserves it right to accept, reject or suggest for modifications on the proposed solution. MSI may also deploy services of a professional architect to prepare the interior design of the DC premises and carry out the civil / electrical / furniture work.
- III. The site preparation activity to be carried out by the successful bidder would include but not limited to civil work for building interiors, realignment of available space based on requirement and architectural plan, necessary masonry, electrical, carpentry and other works, partitioning, flooring, false ceiling & false flooring as appropriately required, painting work, fire proofing of surfaces, cabling, ducting etc.
- IV. MSI shall be responsible for the overall architectural design, aesthetic considerations, and optimal utilization of allotted space to ensure that the DC location is state-of-the-art facilities in line with the importance of the ASCL project. If any of the requirements are not mentioned in the DPR, MSI should include the same as part of additional/proposal line items to ensure that the requirements and expectations of ASCL are met.
- V. The upkeep, maintenance, repairs etc. of the non-IT infrastructure and items commissioned by MSI as part of site preparation shall be the responsibility of MSI for the period of contract. At no point during the contract period, the facilities and infrastructure should be rendered unrepaired.
- VI. Bidders are advised to visit the site of DC and ascertain the scope of work and activities to be carried out at location for site preparation.
- VII. All necessary costs involved in site preparation to be included in the financial bid of the bidders

ASCL shall provide the location to house the compute and storage infrastructure at the Data Centre facility being built at the Command Control and Communication Centre.

Various ICT equipment to be provisioned and maintained by MSI at the Data Centre is given below.

- I. Only the minimum specifications for the active and passive ICT and Non-ICT components are specified.
- II. MSI may propose Data Centre Virtualization solution for price discovery
- III. MSI shall procure items as provided in the BOM which are required to meet the performance requirements as per the proposed business needs. MSI may also suggest additional components as per the solution requirements.

### 3.12.4 Setting up NOC (Network Operations Centre)/ SOC (Security Operations Centre)

- I. Bidder shall setup NOC/SOC Services in the ICCC to monitor and control the network operations for the entire project
- II. The bidder has to ensure that at minimum two factor authentication based access controls are followed for ICCC operations. The bidder shall ensure that all the staff of ICCC should follow the 2 factor authentication for login to their respective terminals while no application login will require 2F authentication. 2-factor authentication shall provide an additional layer of security and shall make system harder for attackers to gain access to a person's devices and because knowing the user's password alone shall not be enough to pass the authentication check.
- III. Bidder shall choose biometric devices as fingerprint readers for implementing 2FA at every desktop that shall be used together with a knowledge factor like username and password credentials as suitable means to provide an effective 2FA solution
- IV. Bidder shall provide 2F authentication application and support to manage both application and biometric devices for additional authentication at desktop login level. All the employees of ICCC shall be supported by MSI for managing authentication to login in their respective terminals.
- V. Bidder shall be responsible for supply, installation, configuration, testing, commissioning, operations and maintenance of network infrastructure items such as Router (cum Firewall), user Layer switches for monitoring
- VI. The NOC/SOC will analyse network problems, perform troubleshooting, communicate with various state site technicians and track problems through resolution. The key objective of the NOC is to ensure the health and availability of components and services.
- VII. When necessary, NOC will escalate problems to the appropriate stakeholders. For emergency conditions, such as a power failure of the NOC, procedures will have to be in place to immediately contact technicians to remedy the problem
- VIII. The bidder shall develop Services catalogue for NOC/SOC and get a sign-off from ASCL.
- IX. Primary responsibilities of NOC personnel shall include but not limited to:
  - a. Network monitoring and management
  - b. Resolution Management including incident and problem management
  - c. Service level management
  - d. Service Continuity and Availability Management
  - e. Reporting
  - f. Root Cause Analysis
  - g. Remediation plans
  - h. SLA monitoring

### 3.12.5 Disaster Recovery and DR Cloud

Provisioning of Disaster Recovery site is not in the scope of the existing phase. It is expected that MSI will build an architecture for DC with due consideration that in subsequent phases, ASCL shall opt for a Disaster Recovery Site

Note: Currently the Surveillance Solutions shall be backed up over tapes locally

### 3.12.6 Application Design, Development, Procurement, Delivery, Configuration, Implementation, Testing, Commissioning, Operations & Maintenance

#### a. Systems Requirement Study & Solution Design

##### Solution Study

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

##### Solution Design

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

##### Development/ Configuration / Work Around for ASCL Smart Solutions

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

##### Solution Testing

- I. The Master System Integrator shall design the Testing strategy including traceability matrix, test cases and conduct testing of various components of the software developed/ configured for the Project
- II. The software testing shall include but not limited to Unit Testing, System Testing, Performance Testing, Integration Testing etc.

- III. The Master System Integrator shall perform the testing of the solution based on the test plan approved by ASCL
- IV. The Master System Integrator shall document the results and shall fix the bugs/ errors found during the testing
- V. It is the ultimate responsibility of Master System Integrator to ensure that the end product delivered meets all the requirements (including functional and technical requirements) specified in the DPR
- VI. The basic responsibility of testing the solution lies with the Master System Integrator.

#### Deployment of ASCL Smart Solution Application

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

#### User Acceptance Testing

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

#### Comprehensive Training

- I. Master System Integrator shall be required to provide training to all the ASCL staff or relevant stakeholders, to enable them to effectively operate and perform the relevant services using the solutions enabled by ASCL
- II. The training content shall have to be relevant to the target trainees depending upon the role played by them i.e. processing hands, technical/ administration personnel, supervisors/ managers, and senior officers etc.
- III. The Master System Integrator shall also be responsible for re-training the selected employees whenever major changes are made in the ASCL Smart Solutions
- IV. The Training shall be conducted in full synchronization with the overall Project Implementation plan

V. Master System Integrator shall prepare a detailed training plan, including the method/ mode of training, training needs at various levels, the proposed curriculum, locations, material, duration of each training program and the entry and exit level criteria, and get it approved by ASCL before starting on the actual training

VI. The language for training shall be both English and Punjabi

#### Ownership and Licenses

- I. The bidder shall provide licenses (perpetual) for application and all system software without constraints
- II. All licenses shall be provided with lifetime validity and free updates/ upgrades/ patches during warranty and AMC period
- III. The ownership of application and all system software designed, developed, procured, delivered, configured, and implemented for the Project shall lie with the ASCL
- IV. All licenses would be in the name of "Amritsar Smart City Limited"

#### b. Provisioning of Hosting/ Co-location Facilities for DC

Master System Integrator shall provision and provide Hosting/ Co-location facilities for DC. The Hosting/ Co-location facilities shall have minimum following:

- I. Tier 3 Data centres for the DC
- II. DRC, when in scope in subsequent phases, shall be in different seismic zone from DC

#### c. Procurement and Installation of IT Infrastructure at DC and Helpdesk

Establishment of IT Infrastructure at the DC and Helpdesk

The Master System Integrator shall procure and implement IT Infrastructure at DC that can suitably meet requirements of performance, security, scalability and availability of ASCL. The hardware set up by the Master System Integrator shall have minimum following:

- I. Standard technologies
- II. Guaranteed Service Levels
- III. High quality support, operations and monitoring of ASCL Smart Solution
- IV. Data and Application availability seven days a week twenty-four hours a day
- V. Facility for centralized management
- VI. Custom security options, multiple security levels
- VII. Backup and archival services

Establishment of Test (Staging) & Development Environment

- I. It is proposed that the Test (staging) & Development environment architecture should be exactly similar to that of production environment
- II. All the components of the Test (staging) & Development environment application should be deployed in the similar way as they are deployed in the production environment (taking care of aspects such as clustering, integration etc.) This would

streamline the process of testing before deployment on the production environment

#### Procurement of IT Infrastructure

- I. The Master System Integrator shall ensure that all the equipment procured is brand new and is free of any defect of any sort
- II. All the hardware should be from reputed OEMs and should come with the appropriate OEM certification, stating that the latest generation of the equipment (No IT equipment model should have been introduced in the market not later than 2 years back as on date of submission of bid) is being provided for the ASCL Smart Solution at the time of deployment
- III. It is expected that Master System Integrator and OEM shall ensure that the equipment/ components being supplied by Master System Integrator shall be supported for minimum 6 years from date of bid submission. If the same is de-supported by the OEM for any reason whatsoever, the Master System Integrator shall replace it with an equivalent or better substitute acceptable to ASCL without any additional cost to the ASCL and without impacting the performance of the ASCL Smart Solution in any manner whatsoever.
- IV. No Products/ equipment under the DPR should be end of life for the Project term

#### IT Infrastructure Installation

- I. The Master System Integrator shall be responsible for Installation and Operationalization & Maintenance of the end-to-end solution, which includes installation of IT Infrastructure at DC
- II. Implementation of SLA Monitoring & Measurement System
- III. Master System Integrator shall design/ procure, implement/ customize the Enterprise Management System (EMS) and shall develop additional tools, if required, to measure performance against each of the indicators listed under SLAs specified in the DPR
- IV. Master System Integrator shall ensure that proposed SLA monitoring system addresses all the SLA measurement requirements and enables calculation of eligible compensation to the Master System Integrator on a quarterly basis, including the penalties as specified in the SLA

#### Warranty

- I. The Master System Integrator shall warrant that the IT Infrastructure procured for the Project shall have no defects arising from design or workmanship or any act or omission. The warranty shall remain valid for project term.
- II. The Master System Integrator warrants that the goods supplied under the DPR are new, non-refurbished, unused and recently manufactured; shall not be nearing End of sale/ End of support; and shall be supported by the Master System Integrator and respective OEM along with service and spares support to ensure its efficient and effective operations for the Project Term

- III. The Master System Integrator shall provide the warranty for IT Infrastructure (Software & hardware) supplied for Project Term on all the items supplied as per the Contract
- IV. The Master System Integrator shall replace any parts/ components of the IT Infrastructure supplied for the Project if the components are defective and during the entire warranty period, Master System Integrator shall apply all the latest upgrades/ patches/ releases for the software after appropriate testing

#### Documentation

- I. The Master System Integrator shall undertake preparation of documents including that of Infrastructure solution design & architecture, configuration files of the Infrastructures, Standard Operating Procedures, and Information Security Management procedures as per acceptable standards
  - II. The Master System Integrator shall take sign-off on the documents, including design documents, Standard Operating Procedures, Security Policy & Procedures from ASCL and shall make necessary changes as recommended by ASCL before submitting the final version of the documents
  - III. Master System Integrator would prepare and submit all the documentation before 'Effective Date of Go-Live' and also ensure that a periodic revision of the documents are also done and submitted to ASCL
- d. Security of Information and Data at DC
- I. The Master System Integrator shall develop a detailed security policy and supporting procedures for the ASCL Smart Solution and obtain ASCL approval to ensure confidentiality, integrity and availability of data. The Master System Integrator shall depute at least one designated Information security expert to be assisted by an additional expert. He shall coordinate with ASCL's Nodal Officer responsible for information security matters. It shall be the responsibility of the Master System Integrator to provide the required equipment, software and other resources to establish the processes and comply with the security requirements of the Solution. The Master System Integrator shall maintain a checklist for tracking the progress of the various activities defined in this DPR.
- e. Technology Refresh
- I. Bidder shall be responsible for performing a feasibility study, prepare an improvement plan and implement the same. This is part of the overall responsibility of bidder for TCO reduction end to end Project operations.
  - II. Response Solution.
  - III. Bidder has to propose first Technology Refresh Reports at the end of 2nd year and in the end of the Contract period.
- f. Requirement for Adherence to Standards
- I. The envisaged ASCL Smart Solution needs to be designed based on a prescribed set of Standards (as illustrated in Table below). These Standards would apply to all the aspects of the envisaged system including (but not limited) Design, Development, Procurement, Delivery, Configuration, Implementation, Testing, Data Migration, Commissioning, Operations & Maintenance and it is essential that the same are achieved and fully-adhered to during application maintenance period.

### Preference for Open Standards

- I. The application must be designed following open standards, to the extent feasible and in line with overall system requirements set out in this DPR, in order to provide for good interoperability with multiple platforms and avoid any technology or technology provider lock-in.

### Compliance with Industry Standards

- I. In addition to above, the proposed solution has to be based on and compliant with industry standards (their latest versions as on date) wherever applicable. There are many standards that are indicated throughout this DPR as well as summarized below. The list below is just for reference and is not to be treated as exhaustive.

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

### g. Acceptance Testing

#### Acceptance Testing & Audit

- I. The primary goal of Acceptance Testing, Audit is to ensure that the solution meets Requirements, Standards, and Specifications as set out in the DPR and as needed to achieve the desired Output, Outcomes and Service Levels. The basic approach for this shall be ensuring that the following are associated with clear and quantifiable metrics for accountability:

- a. Functional requirements
- b. Availability of services in the defined locations
- c. Performance
- d. Security
- e. Manageability

- f. SLA Reporting System
  - g. Project Documentation
- II. Complete testing of the solution shall be performed by Master System Integrator which includes but not limited to preparation of test script and running of test scripts. Master System Integrator has to get approved the same from ASCL.
- III. As part of Acceptance testing & audit, ASCL at any time may review all aspects of project development and implementation of ASCL Smart Solution including the processes relating to the design of solution and sub-systems, coding, testing, business process description, documentation, version control, change management, security, and performance in relation to defined requirements, interoperability, scalability, availability and compliance with all the technical and functional requirements of the DPR

#### Infrastructure Compliance

- I. ASCL may perform the Infrastructure Compliance Review to verify the conformity of the Infrastructure supplied by the Master System Integrator against the requirements and specifications provided in the DPR and/ or as proposed in the proposal submitted by Master System Integrator
- II. Compliance review shall not absolve the Master System Integrator from ensuring that proposed infrastructure meets the SLA requirements

#### Security

- I. ASCL Smart Solution developed by the Master System Integrator shall be tested from security & controls perspective. Such testing shall also include the Application, IT Infrastructure and Network deployed for the ASCL Smart Solution. Following are the broad activities to be performed as part of Security Testing. The security testing shall subject the ASCL Smart Solution for the following activities:
  - a. Audit of Server and Application security mechanisms
  - b. Assessment of authentication mechanism provided in the application/ components/ modules
  - c. Assessment of data encryption mechanisms implemented for the solution
  - d. Assessment of data access privileges, retention periods and archival mechanisms
  - e. Server and Application security features incorporated etc.

#### Performance

- I. Performance is another key requirement for the ASCL Smart Solution and the Master System Integrator shall perform the Performance Testing of the deployed Solution against key parameters defined in SLA described in this DPR and/ or Contract between ASCL and Master System Integrator. Such parameters include request response time, work-flow processing time, concurrent sessions supported by the system. The performance review also includes verification of scalability provisioned in the application for catering to the requirements of volume growth in future.

## Availability

- I. The application should be designed to remove all single point failures. Appropriate redundancy shall be built into all the critical components to provide the ability to recover from failures. ASCL shall perform various tests including server, security, DC failover tests to verify the availability of the services in case of component/location failures.

## Manageability Review

- I. Master System Integrator shall verify the manageability of the ASCL Smart Solution and its supporting sub-systems deployed using any enterprise management system proposed by the Master System Integrator. The manageability requirements such as remote monitoring, administration, configuration, inventory management, fault identification etc. shall have to be tested out.

## SLA Reporting System

- I. Master System Integrator shall develop/ procure/ customize and implement tools required to monitor the performance indicators listed under SLA prescribed in the DPR and calculations of scores accordingly
- II. The Master System Integrator shall verify the Accuracy and Completeness of the information captured by the SLA monitoring system implemented shall certify the same
- III. The Master System Integrator shall provide complete access to ASCL of the SLA tool(s).

## Project Documentation

- I. Master System Integrator shall submit the Project documents developed by Master System Integrator including requirements, design, source code, installation, training and administration manuals, version control etc. Any issues/ gaps identified by ASCL, in any of the above areas, shall be addressed to the complete satisfaction of ASCL.

### 3.12.7 Compliance to SLA

The Master System Integrator shall ensure compliance to uptime and performance requirements of the Solution as indicated in the DPR and any upgrades/ major changes to the Solution shall be accordingly planned by Master System Integrator for ensuring the SLA requirements

### 3.12.8 Application Maintenance

- I. The Master System Integrator shall address all the errors/ bugs/ gaps in the functionality offered by solution (vis-à-vis the FRS or SRS or SDD signed off for Project) at no additional cost during the maintenance period
- II. For performing of any functional changes to system that are deviating from the signed-off FRS or SRS or SDD, a separate Change Control Note (CCN) shall be prepared by Master System Integrator and the changes in the software shall be

- implemented accordingly. The time period for implementation of change shall be mutually decided between the Master System Integrator and ASCL.
- III. Modifications in the delivered ASCL Smart Solutions shall not be considered as Change request, only new requirement shall be considered as change request
  - IV. It is clarified that changes in Application, hardware and other IT Infrastructure required as a result of any legislative, administrative, policy changes by ASCL and workflow shall not constitute change of 'Scope of Work'
  - V. In case there is a change request in the Scope of Work, the Master System Integrator shall prepare the "CNS (change note on Scope of Work)" and get it approved by the department for the additional cost, effort and implementation time
  - VI. The decision of ASCL on change being a CCN or CNS would be final & binding on Master System Integrator

### 3.12.9 Problem identification and Resolution

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

### 3.12.10 Application Change & Version Control

- I. All planned changes to the ASCL Smart Solutions shall be coordinated within established Change Control processes to ensure that:
  - a. Appropriate communication on change required has taken place
  - b. Proper approvals have been received
  - c. Schedules have been adjusted to minimize impact on the production environment
- II. The Master System Integrator shall define the Software Change Management & Version control process and obtain approval for the same from ASCL. For any changes to the ASCL Smart Solutions, Master System Integrator has to prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/ additional features added to the system etc. Master System Integrator is required to obtain approval from ASCL for all the proposed changes before implementation of the same into production environment and such documentation is subject to review at the end of each quarter of operations & maintenance support.

### 3.12.11 Maintain configuration information

- I. Maintain version control and configuration information for application software and any system documentation

### 3.12.12 Maintain configuration information

Maintain and update documentation of the software system. Ensure that:

- I. Application documentation is updated to reflect on-going maintenance and enhancements including but not limited to FRS, SRS, SDD and RTM
- II. User manuals & training manuals are updated to reflect on-going changes/ enhancements
- III. Standard practices are adopted & followed for version control and management

### 3.12.13 Provide Change Control

All planned changes to application shall be coordinated within established Change control processes to ensure that:

- I. Appropriate communication on change required has taken place
- II. Proper approvals have been received

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

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

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

### 3.13 Design and Implementation of Disaster Recovery Infrastructure for ICCC project

- I. MSI shall propose to host Applications and storage on cloud for complete Data Recovery (DR) operations. Applications should fail-over to the cloud in case of DR. The MSI should design the DR according to RTO/RPO as mentioned below:

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

- II. DR shall be implemented based on managed cloud services and shall adhere to guideline issued by MeitY over time to time. SLA for DR shall be as per MeitY guideline.
- III. MSI may propose the Cloud Service Provider from the empanelled vendors of MeitY.
- IV. Below are the key factors to be considered for cloud hosting -
- The MSI is required to prepare and submit along with their technical proposal, the details of methodologies and computations for sizing and capacity of storage, compute, backup, network and security.
  - There should be logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers on Private cloud.
  - The cameras shall operate at lower settings i.e. 720P @ 10 FPS in case of DR scenario. This setting profile shall be applied by VMS on cloud on field cameras to reduce bitrate in DR scenario. ANPR cameras shall operate at 720p@ 25 FPS.
  - All applications in scope shall be operational from DR site after DC is not available as per RTO/RPO guideline.
  - Viewing bandwidth shall be provisioned for minimum of 100 cameras streams at one time in DR scenario. During the period of disaster it shall be possible to view video feeds from multiple police viewing centres in the city.
  - All the important video evidence shall be moved to unified storage on regular basis with help police personnel (ideally within 7 days). The complete application databases, tagged video evidence data and other important data and files on 125 TB unified storage shall be replicated in cloud on based on RPO/RTO guidelines. It shall be duty of MSI to delete data after requisite permissions from police department.
  - All applications except Face Recognition shall be operational
  - The camera stream to DR shall be activated only in DR Scenario to reduce bandwidth cost.
  - It is expected that bidder shall make all necessary provision to ensure high availability at the Data Centre and after switch over to the DR; it gets back in to normal operations from the DC as soon as possible. However, the overall disaster Recovery Solution should be provisioned in such a manner that previous 7 days feeds are available and it should be able to run for 7 Days in case of Disaster.
  - One full-scale DR drill to be conducted during UAT & post go-live and additional DR Drills on quarterly yearly basis shall be conducted. Total DR period in a year shall be assumed to be 24 days a year for purpose of sizing including DR drills
  - The system shall be hosted in the site identified by the MSI and as agreed by the ASCL for DR in a different seismic zone.

- There should be sufficient capacity (compute, network and storage capacity offered) available for near real time performance (as per the SLA requirement of the ASCL) during any unanticipated spikes in the user load.
  - DR site shall be located in India only.
  - The design ensure redundancy at each level
  - MSI shall provide interoperability support with regards to available APIs, data portability etc. for the ASCL to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
  - The MSI is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the MSI.
  - ASCL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the ASCL's application. ASCL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time
  - Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.999%, SLA measured at the VM Level & SLA measured at the Storage Levels
  - Cloud services should be accessible via internet and MPLS.
  - Required Support to be provided to the ASCL in migration of the VMs, data, content and any other assets to the new environment created by the ASCL or any Agency (on behalf of the ASCL) on alternate cloud service provider's offerings to enable successful deployment and running of the ASCL's solution on the new infrastructure.
  - The MSI should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications
  - Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
  - For the files, perform weekly backups;
  - For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
  - Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.
  - Retain database backups for thirty (30) days
- V. The MSI should offer dashboard to provide visibility into service via dashboard.
- VI. MSI shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the approval of the ASCL.

## Preparation of Disaster Recovery Operational Plan

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

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

Configure proposed solution for usage

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

Periodic Disaster Recovery Plan Update

The service provider shall be responsible for -

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

### [3.13.1 Preparation of Disaster Recovery Operational Plan](#)

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

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

### [3.13.2 Configure proposed solution for usage](#)

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

S .No.	Minimum Requirement Description
1	The proposed solution must offer a workflow based management & monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts( including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment.

S .No.	Minimum Requirement Description
	This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, and Unix etc. with high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

### 3.13.3 Periodic Disaster Recovery Plan Update

The service provider shall be responsible for

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

#### 4. Project Implementation Timelines, Deliverables and Payment Terms

S.N o	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
1.	Project Award and Contract Signing between ASCL and successful Bidder	Project Start Date = T0		-
2.	Performance Bank Guarantee (PBG)		Performance Bank Guarantee (PBG) for the Project Term	-
3.	Team Deployment for the following: • Project Planning • Resource Scheduling • Development, Implementation & Maintenance approach	T0 + 0.5	• Final Project Plan • Project Inception Report	-
4.	Submission and approval of Site-survey Report (All tracks)	T0 + 2	• Solution Design Document • Final Survey Reports	5 % of the CAPEX
5.	Completion of Site preparation, Civil Works, HVAC Systems, Furniture and Electrical Work of Data Centre and ICCC	T0 + 6	• Completion Reports • Inspection Reports approved by ASCL	15 % of the CAPEX
6.	Supply of all equipment/ components (Hardware) including System Software Licenses at the Data Centre and ICCC	T0 + 6.5	• Delivery Challan with date & stamp on delivery proof • Copy/Original excise duty gate-pass • Inspection report from an authentic third party • Warranty certificate issued by respective OEMs for each hardware back to back in the name of "ASCL" • License in case of system software • Manufacturer Authorization Form • Country of origin certificate	10 % of the CAPEX
7.	Supply of all field equipment/ components (Hardware) including System Software Licenses	T0 + 7	• Delivery Challan with date & stamp on delivery proof • Copy/Original excise duty gate-pass • Inspection report from an authentic third party • Warranty certificate issued by respective OEMs for each hardware back to back in the name of "ASCL"	10 % of the CAPEX

S.N o	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
			<ul style="list-style-type: none"> <li>• License in case of system software</li> <li>• Manufacturer Authorization Form</li> <li>• Country of origin certificate</li> </ul>	
8.	Installation, Testing, Configuration and Operationalization of all equipment/components (Hardware) including system software licenses at the Data Centre and ICCC	T0 + 8.5	<ul style="list-style-type: none"> <li>• Device-wise configuration report stating IP schema</li> <li>• Installation, Testing and Commissioning Report</li> <li>• Complete set of Technical, Operations &amp; Maintenance Manual</li> <li>• Configuration Change Report</li> <li>• Software Installation Guide and Checklist</li> <li>• Insurance certificate from the Insurance Company</li> </ul>	15 % of the CAPEX
9.	Installation, Testing, Configuration and Operationalization of all field equipment including System Software Licenses	T0 + 10	<ul style="list-style-type: none"> <li>• Device-wise configuration report stating IP schema</li> <li>• Installation, Testing and Commissioning Report</li> <li>• Complete set of Technical, Operations &amp; Maintenance Manual</li> <li>• Configuration Change Report</li> <li>• Software Installation Guide and Checklist</li> <li>• Insurance certificate from the Insurance Company</li> </ul>	15 % of the CAPEX
10.	User Acceptance Testing, Training and Go-Live of all smart components	T0 + 12	<ul style="list-style-type: none"> <li>• UAT Report</li> <li>• Training and Capacity Building</li> <li>• Defect Resolution Report</li> <li>• Commissioning Report</li> <li>• User Acceptance Testing and Go-Live of all Smart Solutions</li> </ul>	10 % of the CAPEX
11.	Post Go-Live Support		<ul style="list-style-type: none"> <li>• SLA Adherence Report on a Monthly/ Quarterly basis</li> </ul>	CAPEX amortized over 4 years: 20% (16 quarterly payments of 1.25% after in equated instalments after deductions of SLA)

S.N o	Activity / Task	Timelines (Months)	Deliverables / Milestone	Payment Milestone
				penalties)  AND  OPEX amortized for 4 years payable quarterly at the end of each quarter in equated instalments after deductions of SLA penalties

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

## 5. Service Level Agreement

### 5.1 Purpose

- I. The purpose of Service Levels is to define the levels of service provided to the MSI by the Client for the duration of the contract. The benefits of this are:
- II. Help the Client control the levels and performance of SI services;
- III. Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.
- IV. The Service Levels are between the Client and MSI.

### 5.2 Service Level Agreement & Targets

- I. This section is agreed to by Client and MSI as the key performance indicator for the project;
- II. The following section reflects the measurements to be used to track and report systems performance on a regular basis. The targets shown in the following tables are for the period of Contract.

#### General Principles of Service Level Agreement

- I. Service Level Agreement (SLA) shall become the part of the Contract between the Client and the MSI. SLA defines the terms of SI's responsibility in ensuring the timely delivery of the deliverables and the correctness of the deliverables based on the agreed performance indicators as detailed in this section.
- II. The MSI shall comply with the SLAs to ensure adherence to project timelines, quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
  - "Total Time" – Total number of hours in consideration for evaluation of SLA performance.
  - "Downtime" – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the MSI.
  - "Scheduled Maintenance Time" – Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The MSI shall take at least 7 days prior approval from the Client for any such activity. The scheduled maintenance should be carried out during nonpeak- hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.
  - "Uptime" – Time period for which the specified services are available in the period being considered for evaluation of SLA.
  - Uptime (%) =  $[1 - \{(Total Downtime) / (Total Time - Scheduled Maintenance Time)\}] * 100$ .
  - "Availability": When the system is working properly performing all business and functional requirements as defined in this DPR.

- Availability = ((Agreed Hours - (Incident(s) x Duration)) / Agreed Hours)\*100
- Penalties shall be applied for each criteria individually and then added together for the total penalty for a particular quarter.
- "Incident" – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.
- "Response Time" – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.
- "Resolution Time" – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

### 5.3 Measurement & Target

- a. Implementation Phase related SLAs
  - i. During Implementation phase any delay in deliverables and milestones shall attract liquidated damages as per conditions of Contract.
- b. Operations & Maintenance Phase related SLAs
  - i. These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and commencement of the O&M Phase. These SLAs and associated performance shall be monitored on quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.
  - ii. The Scheduled Maintenance Time should be approved by the client in writing. The schedule maintenance request should be submitted to the client 15 days in advance from the scheduled maintenance rate.
  - iii. The Exhibit below provides the Service Level's (SLA) to be adhered by the bidder during the operational hours of the project/system/sub-system/components. The scheduled maintenance and the scheduled down time shall be carried out by the Bidder during the non-operational hours of the project. In case of not meeting the SLA's, the corresponding penalties as defined in the Exhibit in the subsequent section on next page:
- c. Severity Weights
  - i. "Upon ninety (90) days' advance notice to Master System Integrator, ASCL may adjust the Severity Weights of the respective Service Levels, as ASCL deems appropriate, so long as the total of such percentages does not exceed one hundred percent (100%)."
- d. Service Level Changes
  - i. From time to time, ASCL may add or delete Service Levels or assign or adjust Severity Weights, but the aggregate of all Severity Weights may not exceed 100% within a Service Category. New Service Levels are Changes authorized through the Change Control Procedures. Changes that add Service Levels shall be effective within ninety (90) days after ASCL proposes the Change, or as otherwise agreed.

## 5.4 Implementation SLA Matrix

S.No	Activity / Task	Timelines (Months)	Deliverables / Milestone	Penalty
1.	Project Award and Contract Signing between ASCL and successful Bidder	Project Start Date =T0		NA
2.	Performance Bank Guarantee (PBG)		Performance Bank Guarantee (PBG) for the Project Term	NA
3.	Team Deployment for the following: • Project Planning • Resource Scheduling • Development, Implementation & Maintenance approach	T0 + 0.5	• Final Project Plan • Project Inception Report	NA
4.	Submission and approval of Site-survey Report (All tracks)	T0 + 2	• Solution Design Document • Final Survey Reports	10 % of the Invoice Amount
5.	Completion of Site preparation, Civil Works, HVAC Systems, Furniture and Electrical Work of Data Centre and ICCC	T0 + 6	• Completion Reports • Inspection Reports approved by ASCL	10 % of the Invoice Amount
6.	Supply of all equipment/ components (Hardware) including System Software Licenses at the Data Centre and ICCC	T0 + 6.5	• Delivery Challan with date & stamp on delivery proof • Copy/Original excise duty gate-pass • Inspection report from an authentic third party • Warranty certificate issued by respective OEMs for each hardware back to back in the name of "ASCL" • License in case of system software • Manufacturer Authorization Form • Country of origin certificate	10 % of the Invoice Amount

S.No	Activity / Task	Timelines (Months)	Deliverables / Milestone	Penalty
7.	Supply of all field equipment/ components (Hardware) including System Software Licenses	T0 + 7	<ul style="list-style-type: none"> <li>• Delivery Challan with data &amp; stamp on delivery proof</li> <li>• Copy/Original excise duty gate-pass</li> <li>• Inspection report from an authentic third party</li> <li>• Warranty certificate issued by respective OEMs for each hardware back to back in the name of "ASCL"</li> <li>• License in case of system software</li> <li>• Manufacturer Authorization Form</li> <li>• Country of origin certificate</li> </ul>	10 % of the Invoice Amount
8.	Installation, Testing, Configuration and Operationalization of all equipment/components (Hardware) including system software licenses at the Data Centre and ICCC	T0 + 8.5	<ul style="list-style-type: none"> <li>• Device-wise configuration report stating IP schema</li> <li>• Installation, Testing and Commissioning Report</li> <li>• Complete set of Technical, Operations &amp; Maintenance Manual</li> <li>• Configuration Change Report</li> <li>• Software Installation Guide and Checklist</li> <li>• Insurance certificate from the Insurance Company</li> </ul>	10 % of the Invoice Amount
9.	Installation, Testing, Configuration and Operationalization of all field equipment including System Software Licenses	T0 + 10	<ul style="list-style-type: none"> <li>• Device-wise configuration report stating IP schema</li> <li>• Installation, Testing and Commissioning Report</li> <li>• Complete set of Technical, Operations &amp; Maintenance Manual</li> <li>• Configuration Change Report</li> <li>• Software Installation Guide and Checklist</li> <li>• Insurance certificate from the Insurance Company</li> </ul>	10 % of the Invoice Amount
10.	User Acceptance Testing, Training and Go-Live of all smart components	T0 + 12	<ul style="list-style-type: none"> <li>• UAT Report</li> <li>• Training and Capacity Building</li> <li>• Defect Resolution Report</li> <li>• Commissioning Report</li> <li>• User Acceptance Testing and Go-Live of all Smart Solutions</li> </ul>	10 % of the Invoice Amount

## 5.5 Operations SLA Matrix

All Operations & Maintenance SLA shall be monitored by MSI using EMS and NMS tools and providing reports for the same shall be in scope of the MSI. MSI shall also be responsible for building any custom reports required by ASCL by interfacing to applications, database, API , logs or other interfaces for correct reporting for all metrics related to SLA's provided below. ASCL or a third party auditor reserves the right to decide the method for calculation of the SLA provided below and make any corrections to methods used.

### 5.5.1 Data Hosting & IT Infrastructure at ICCC

**"Data Hosting & IT Infrastructure Availability":** When the system is working properly performing all business and functional requirements as defined in this RFP.

**Measurement Tool:** Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

**"UPS Availability"** is defined as: When UPS is available in full working condition as defined in this RFP. UPS running in "Bypass" mode shall also be considered as unavailable. Availability shall be calculated only for power outages that are less than the UPS backup time. Power outages beyond UPS backup time shall be excluded from the SLA calculations.

S. No	Component	Severity Level	Requirement	Falls By / Increases By	Penalty (INR)	Calculation (Currency in INR)
1.	Servers / Storage /Router/ Switches/ Link Load Balancers	High	99.90%	0.10%	50000	For every decrease of 0.10% in availability of each device & its associated components in a quarter, a penalty of 50000 shall be imposed on quarterly payment
2.	Firewall / IPS/ AMP/ APT// DDOS/ WAF	High	99.90%	0.10%	50000	For every decrease of 0.10% in availability of each device & its associated components in a quarter, a penalty of 100000 shall be imposed on quarterly payment

S. No	Component	Severity Level	Requirement	Falls By / Increases By	Penalty (INR)	Calculation (Currency in INR)
3.	Workstations/Laptops/Multifunctional Printer /Monitors/IP Phones/Joy Stick	Moderate	99%	0.50%	5000	For every decrease of 0.50% in availability of each device & its associated component in a quarter, a penalty of 5000 shall be imposed on quarterly payment
4.	ICCC Software Platform	High	99.50%	0.50%	7500	For every decrease of 0.50% in availability of the ICCC Software Platform & its associated services in a quarter, a penalty of INR 7500 for every 0.50% decrease shall be imposed on quarterly payment
5.	Video Wall & Management System	High	99.90%	0.10%	20000	For every decrease of 0.10% in availability of Video wall & its Management System in a quarter, a penalty of INR 20000 shall be imposed on quarterly payment
6.	Building Management system	High	99.50%	0.50%	7500	For every decrease of 0.50% in availability of the Building Management system & its associated services in a month, a penalty of INR 7500 for every 0.50% decrease shall be imposed on quarterly payment
7.	Access management system	High	99.50%	0.50%	7500	For every decrease of 0.50% in availability of Access management system & its associated component in

S. No	Component	Severity Level	Requirement	Falls By / Increases By	Penalty (INR)	Calculation (Currency in INR)
						a month, a penalty of INR 7500 shall be imposed on quarterly payment
8.	UPS	Medium	99.90%	0.10%	10000	For every decrease of 0.10% in Uptime of each UPS in a month, a penalty of INR 5000 shall be imposed
9.	Diesel Generators	High	99.90%	0.10%	10000	For every decrease of 0.10% in Uptime of the Diesel Generators & its associated services in a month, a penalty of INR 7500 for every 0.50% decrease shall be imposed on quarterly payment
10.	Manpower	Low	Man power / shift	Shift	3000	Non availability of resource INR 3000/ Man power/shift shall be deducted from quarterly payment
11.	Sitting enclosures , chairs, tables, fans, AC. Lights, light enclosures or any other equipment/devices and other Non-IT hardware at ICCC	Low	Within 48 hours	Day	500	INR 500 for every day after 48 hours shall be deducted quarterly payment
12.	Safety Equipment like Fire Extinguishers and their refilling	High	Within 24 Hours	Day	5000	INR 5000 for every day after 24 hours shall be deducted quarterly payment

## 5.5.2 Communication Network

### 5.5.2.1 Performance levels for leased Network

Mean Time to Repair (MTTR) shall be monitored on the time taken between logging of complaint against the network and its closure.

Measurement Tool: Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

S. No.	Component	Severity Level	Requirement	Falls By / Increases By	Penalty (INR)	Calculation
1.	Mean Time to repair	High	4 hours	Hour	20000	For every hour after 4 hours, a penalty of INR 20000 shall be imposed on quarterly payment
2.	Uptime	High	99.9%	0.1%	25000	For every 0.1% decrease in uptime below requirement , a penalty of INR 20000 shall be imposed on quarterly payment
3.	Network Latency	High	< 50 ms Round Trip	1 ms	25000	For every incident of increase in latency above 50 ms, a penalty of INR 25000 shall be imposed on quarterly payment
4.	Jitter	High	< 5 ms	1ms	25000	For every incident of increase in jitter above 5 ms, a penalty of INR 25000 shall be imposed on quarterly payment
5.	Packet Loss	High	< 0.1%	.01%	25000	For every incident of increase in packet loss above .1% , a penalty of INR 25000 shall be imposed on quarterly payment
6.	Available Bandwidth at Junction Box	High	100%	1%	25000	For every incident of 1% decrease in available bandwidth at each junction box level, a penalty of INR 25000 shall be imposed on quarterly payment

S. No.	Component	Severity Level	Requirement	Falls By / Increases By	Penalty (INR)	Calculation
6.	Available Bandwidth at ICCC	High	100%	1%	25000	For every incident of 1% decrease in available bandwidth at ICCC, a penalty of INR 25000 shall be imposed on quarterly payment

### 5.5.3 Security SLA

S. No.	Component	Severity Level	Requirement	Fall By / Increases By	Penalty (INR)	Calculation
1.	Security Reporting	High	Quarterly security report to be submitted with 100% KPIs defined for security (agreed with Client at start of project)	1 day	2000	For every delay of one day a penalty of INR 2000/day shall be imposed
2.	Vulnerability assessment and closure	High	Vulnerability assessment for all systems/subsystems shall be performed at least once every quarter and all detected vulnerabilities to be closed within 7 days. Client may appoint third party agency to cross-check.	1 day	2000	For every delay of one day after 7 days a penalty of INR 2000/day shall be imposed
3.	Penetration Testing	High	Penetration testing shall be conducted once every quarter. All vulnerabilities shall be closed within 7 days.	1 day	2000	For every delay of one day after 7 days a penalty of INR 2000/day shall be imposed
4.	Application Security	High	Cyber Crime/Hacking/Data Theft/Fraud shall be attributable to MSI To be evaluated per occurrence.	1 day	2000	For every delay of one day a penalty of INR 2000/day shall be imposed

#### 5.5.4 City Surveillance

Measurement Tool: Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

##### Surveillance Network Equipment & Software SLA

S. No.	Component	Severity Level	Requirement	Falls/Increases By	Penalty (INR)	Calculation
<b>IT Component</b>						
1.	Camera (Fixed & PTZ)	High	99.50%	0.10%	5000	For every decrease of 0.10% in uptime of the Camera & its associated services in a month, a penalty of INR 5000 for every 0.10% decrease shall be imposed
2.	IR illuminator	High	99.50%	0.10%	5000	For every decrease of 0.10% in uptime of the IR Illuminators in a month, a penalty of INR 5000 for every 0.10% decrease shall be imposed
3.	16 port POE+ Industrial Switches	High	99.50%	0.10%	5000	For every decrease of 0.10% in Uptime of each 16 port POE+ Industrial Switches in a month, a penalty of INR 5000 shall be imposed
4.	Junction Box (including last mile networking, earth, Power Backup etc.)	High	99.50%	0.10%	5000	For every decrease of 0.10% in Uptime of Junction Box, internal equipment, earthing, etc.) in a month, a penalty of INR 5000 shall be imposed

S. No.	Component	Severity Level	Requirement	Falls/Increases By	Penalty (INR)	Calculation
	IT Component					
5.	Emergency Call Box System	High	99.50%	0.10%	5000	For every decrease of 0.50% in Emergency Call Box, in a quarter, a penalty of INR 5000 shall be imposed
6.	VMS and Video Recording Servers	High	99.9%	0.10%	50000	For every decrease of 0.10% in availability of either VMS or Video Recording in a month, a penalty of INR 50000 shall be imposed
7.	Video Analytics, ANPR or Face Recognition Applications	High	99.5%	0.10%	25000	For every decrease of 0.10% in availability of either Video Analytics, ANPR or Face Recognition Applications in a month, a penalty of INR 25000 shall be imposed
	Non IT Component					
8.	Pole	Medium	99.00%	1.00%	5000	For every decrease of 1.00% in Uptime of each pole in a month, a penalty of INR 5000 shall be imposed

## Surveillance Network Performance SLA

S. No.	Component	Severity Level	Requirement	Fall By/Increase By	Penalty(INR)	Calculation
1.	Mean Time to repair	High	4 hours	1 Hours		For every hour after 4 hours 0.5% of payment shall be deducted from quarterly payments.
2.	End to End Surveillance Camera Streams (Cameras streams to Recording servers and Video Wall)	High	99.9%	0.1%	25000	For every 0.1% decrease in uptime of a camera stream below requirement , a penalty of INR 25000 shall be imposed on quarterly payment
3.	End to End Surveillance Camera Stream Latency	High	< 50 ms Round Trip	1 ms	25000	For every incident of increase in latency above 50 ms a camera stream, a penalty of INR 25000 shall be imposed on quarterly payment
4.	End to End Surveillance Camera Stream Network Jitter	High	< 5 ms	1ms	25000	For every incident of increase in jitter above 5 ms a camera stream, a penalty of INR 25000 shall be imposed on quarterly payment
5.	End to End Surveillance Camera Stream Packet Loss	High	< 0.1%	.01%	25000	For every incident of increase in packet loss above .1% a camera stream, a penalty of INR 25000 shall be imposed on quarterly payment

#### Automatic Number Plate Recognition (ANPR): Performance/Accuracy

"Detection Accuracy": The detection accuracy of an ANPR system is measured against the license plates been detected by the system. Any license plate not correctly detected by ANPR system shall be considered as unreadable and specified penalty shall be applicable.

**"Conversion Accuracy":** The conversion accuracy of an ANPR system is measured against the license plates been correctly converted into alpha numeric format by the system. If any license plate cannot be correctly converted by ANPR system, the specified penalty shall be applicable.

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
1.	ANPR detection Accuracy	High	95%	1%	5000	For every decrease of 1% in detection in a quarter, a penalty of INR 5000 shall be imposed
2.	ANPR conversion Accuracy for Standard Number Plate	Medium	85%	1%	10000	For every decrease of 1% in conversion of number plate by system in a quarter, a penalty of INR 10000 shall be imposed.
3.	ANPR conversion Accuracy for Non-standard Number Plate	Medium	70%	1%	10000	For every decrease of 1% in conversion of number plate by system in a quarter, a penalty of INR 10000 shall be imposed.
4.	Speed Accuracy: should be + 5% w.r.t actual speed of the vehicle	Medium	90%	1%	5000	For every decrease of 1% in speed accuracy by system in a quarter, a penalty of INR 5000 shall be imposed.

#### Face Recognition - Performance/Accuracy

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
1.	Matching of Known Faces from database with full face view	High	95%	1%	20000	For every decrease of 1% in face matching in a quarter, a penalty of INR 20000 shall be imposed

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
2.	Matching of Known Faces from database with partial face view	Medium	75%	1%	20000	For every decrease of 1% in face matching by system in a quarter, a penalty of INR 20000 shall be imposed.
3.	1:N Face matching Speed (Database of 10,000 faces)	High	5 Sec	.1 sec	20000	For every instance of decrease of .1sec in 1: N Face matching by system in a quarter, a penalty of INR 20000 shall be imposed.

## Public Announcement System

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
1.	VoIP/Amplifier with Built-in DSP	High	99%	0.5%	5000	For every decrease of 0.50% in availability of each device & its associated component in a quarter, a penalty of INR 5000 shall be imposed.
2.	PAS Speakers	Medium	99%	0.5%	10000	For every decrease of 0.50% in availability of each device & its associated component in a quarter, a penalty of INR 10000 shall be imposed.
3.	Ambient Noise Sensor	Medium	98%	1%	5000	For every decrease of 1% in availability of each device & its associated component in a quarter, a penalty of INR 5000 shall be imposed.

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
4.	PAS Operator Console	Medium	99%	0.5%	5000	For every decrease of 0.50% in availability of each device in a period of one month, a penalty of INR 5000 shall be imposed
5.	Variable Message Sign (VMS)	High	99%	0.5%	5000	For every decrease of 0.50% in availability of each device & its associated component in a quarter, a penalty of INR 5000 shall be imposed

#### 5.5.5 Environment Sensor

Measurement Tool: Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

S. No.	Component	Severity Level	Requirement	Penalty (INR)	Calculation
1.	Field Air Quality Monitoring Station	High	99.00%	5000 per 1.00% decrease	For every decrease of 0.50% in Availability of the mobile API & web application server & its associated services in a month, a penalty of INR 5000 for every 0.50% decrease shall be imposed
2.	Variable Message Signboard	High	99.00%	10000 per 1.00% decrease	For every decrease of 1% in availability of each device & its associated component in a quarter, a penalty of INR 10000 shall be imposed
3.	Overall Network Availability	High	99.50%	1000 per 0.25% decrease	For every decrease of 0.25% in availability of each device & its associated component in a quarter, a penalty of INR 1000 shall be imposed

S. No.	Component	Severity Level	Requirement	Penalty (INR)	Calculation
4.	Mean Time To Repair (MTTR)	Medium	<= 2 hours	5000 per 30 mins	For every increase of 30 mins in repairing of Fibre / network & its associated component in a quarter, a penalty of INR 50000 shall be imposed
5.	Central Air Quality Monitoring Software	High	99.50%	2500 per 0.50% decrease	For every decrease of 0.50% in Availability of the Central Environment System & its associated services in a month, a penalty of INR 2500 for every 0.50% decrease shall be imposed
6.	Mobile Application	High	99.50%	5000 per 0.50% decrease	For every decrease of 0.50% in uptime of each Mobile Application & its associated component in a month, a penalty of INR 5000 shall be imposed
7.	Manpower	Low	Man power / shift	1000	Non availability of man power. INR 1000/ Man power/shift
8.	Replacement of Manpower	Medium	Manpower as per contract and deployed	1000	INR 1000 for Non Availability of a resource / per day. (INR 1000 per resource/day)

\*All the numbers shall be rounded off to nearest decimal. For e.g. 98.82 shall be rounded off to 98.8 and 98.87 shall be rounded to 98.90.

Note- Hardware, operating systems, IP Monitoring components are expected to be available, functioning and delivering all its expected services to the fullest. The MSI integrator is expected to hold contingency plans, redundant devices , spare parts to ensure 100% uptime and 100% availability of their equipment's and applications so uninterrupted service from each equipment is achieve.

### 5.5.6 Water Quality Analyser

Measurement Tool: Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

S. No.	Component	Severity Level	Requirement	Penalty (INR)	Calculation
1.	BOD , COD , TSS Analyser	Medium	99%	10000	For every decrease of 0.50% in Availability of BOD , COD, TSS Analyser and other associated hardware per location in a month, a penalty of INR 10000 shall be imposed on the quarterly payment
2.	Dissolved Oxygen Analyser	Medium	99%	10000	For every decrease of 0.50% in Uptime of Dissolved Oxygen Analyser and other associated hardware per location in a month, a penalty of INR 10000 shall be imposed on the quarterly payment
3.	PH and Temperature Analyser	Medium	99%	10000	For every decrease of 0.50% in Uptime of PH and temperature analyser and other associated hardware per location in a quarter, a penalty of INR 10000 shall be imposed on the quarterly payment
4.	Ammoniac Nitrogen Analyser (NH4-N)	Medium	99%	10000	For every decrease of 0.50% in Uptime of Ammoniac Nitrogen analyser (NH4-N) and other associated hardware along per location in a quarter, a penalty of INR 10000 shall be imposed on the quarterly payment
5.	Oil and Grease Analyser	Medium	99%	10000	For every decrease of 0.50% in Uptime of Oil and Grease analyser and other associated hardware per location in a quarter, a penalty of INR 10000 shall be imposed on the quarterly payment
6.	Open Channel Embankment Mounted Electrical Control Panel with Intelligent Gateway , Analog-Digital Converter Cards, Integrated	Medium	99%	10000	For every decrease of 0.50% in Uptime of Open Channel Embankment Mounted Electrical Control Panel with Intelligent Gateway , Analog-Digital Converter Cards,

S. No.	Component	Severity Level	Requirement	Penalty (INR)	Calculation
	3G/4G communication, DC SMPS , Cable and Other Accessories (As per Requirement)				Integrated 3G/4G communication, DC SMPS , Cable and Other Accessories per location in a month, a penalty of INR 10000 shall be imposed on the quarterly payment
7.	In-Situ Flotation Buoy with Integrated Sensor Probes and tethering chain from embankment	Medium	99%	10000	For every decrease of 0.50% in Uptime of In-Situ Flotation Buoy with Integrated Sensor Probes and tethering chain from embankment per location in a month, a penalty of INR 10000 shall be imposed on the quarterly payment
8.	OWQMS based Web application	Medium	99%	10000	For every decrease of 0.50% in Availability of OWQMS Cloud Subscription based Web application per location in a month, a penalty of INR 10000 shall be imposed on the quarterly payment
9.	Network Connectivity	Medium	99%	10000	For every decrease of 0.50% in Uptime of Network between Control Panel and ICCC in a quarter, a penalty of INR 7500 shall be imposed on the quarterly payment

#### 5.5.7 Fleet Tracking

Measurement Tool: Reports from EMS & NMS Tools provided to ASCL or its appointed agency by MSI. Third party agency shall audit configuration of EMS & NMS and submitted reports on the performance and adherence to the SLA's on regular basis.

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
1.	AVL OBU	High	99%	0.5%	5000	For every decrease of 0.50% in availability of each device & its associated component in a

S. No.	Component	Severity Level	Requirement	Fall By/Increases By	Penalty (INR)	Calculation
						quarter, a penalty of INR 5000 shall be imposed.
2.	Fleet Tracking Software	High	99%	0.5%	5000	For every decrease of 0.50% in availability of Fleet Tracking Software & its associated components in a quarter, a penalty of INR 5000 shall be imposed.

## 6. Functional Requirement Specifications

### 6.1 Field Infrastructure Functional Requirements

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

### 6.2 City Surveillance

#### 6.2.1 Objectives of strengthening Security Surveillance

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

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

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

S. No.	Location Name	Type of location	
1.		Existing Cameras	All Existing IP Camera Location

S. No.	Location Name	Type of location
2.		Crime Hotspots Major junction where Crime incident usually took place
3.		Procession/Gathering Hotspots Prominent locations where mostly crowd gathering events take place
4.		Traffic Congestion Points All Traffic signals Railway station - inner and outer area with all entry & exit points
5.		City Entry/Exit Points All the entry and exit point of Amritsar
6.		Railway Stations Entry/Exit Points Railway station - inner and outer area with all entry & exit points
7.		Bus Stations Entry/Exit Points The entry and exit point of all the Bus Stations
8.		Airport Entry / Exit Points Entry and exit gate of Amritsar Airport road
9.		Tourist Hotspots Entry/Exit Points All the tourist departments
10.		Main Markets Entry/Exit Points / Prime view All exit and entry point of main market and prime locations
11.		Schools School entry and exit gate
12.		Government Colleges (Entry/Exit Points) Government College entry and exit gate
13.		Government Hospitals All areas around prominent hospitals in the City Prominent commercial area locations and complexes
14.		Traffic Junctions All major traffic junctions of the city
15.		Parking Lots IP Camera for Parking lots
16.		Administrative Building In front of administrative building

S. No.	Location Name	Type of location
17.		Government Infrastructure Assets All Government infrastructure assets.

### 6.2.2 Surveillance System Sub-Components

- I. Surveillance system deployed by MSI shall have IP Cameras that generates real-time video streams, which are monitored, analysed and stored at ICCC for maintaining law and order in the city
- II. The MSI shall deploy Junction boxes at all identified locations to aggregate IP camera feeds and transmit them to ICCC over backhaul network leased from existing ISP's in the city
- III. The MSI shall supply Video Management and Recording application servers at the ICCC to administer the cameras remotely, real-time viewing of the cameras and recording the live video streams for a period of 30 Days for law and order function
- IV. The MSI shall provide both edge and server side video analytics that can be applied to the video streams and alerts can be generated from it to escalate incidents in real-time for quick response
- V. The MSI shall also implement Facial Recognition System (FRS) on 50 video streams to help the agencies deter criminal offences and also safeguard public at airport, railway stations, bus stations, crime hotspots and city entry & exits
- VI. The MSI shall also implement Automatic Number Plate Recognition (ANPR) system on around 72 video streams to help the agencies identify and locate blacklisted vehicles at airport, railway stations, bus stations and city entry & exits
- VII. The MSI shall also implement Emergency Call Box with panic button at around 10 locations to help the citizens to reach the ICCC and facilitate reporting of emergency incidents to police from these locations in the city
- VIII. The MSI shall also implement an IP network based Public Announcement (PA) system at around 25 locations to help the police to control law and order and traffic from ICCC at these locations in the city. These locations shall also have PTZ and other cameras to support remote viewing and check adherence to instructions transmitted over PA system

S. No.	Servers	Description
1.	Video Management Server(s)	Video Management System Servers shall maintain coherent operations between all servers and workstations. It shall host Control Centre, where the system is administered, and System database. It shall monitor one or more Recorder servers on separate dedicated computers, storage devices, IP-compatible devices, and one or more workstation. All network communication shall also be performed via the Video Management servers.

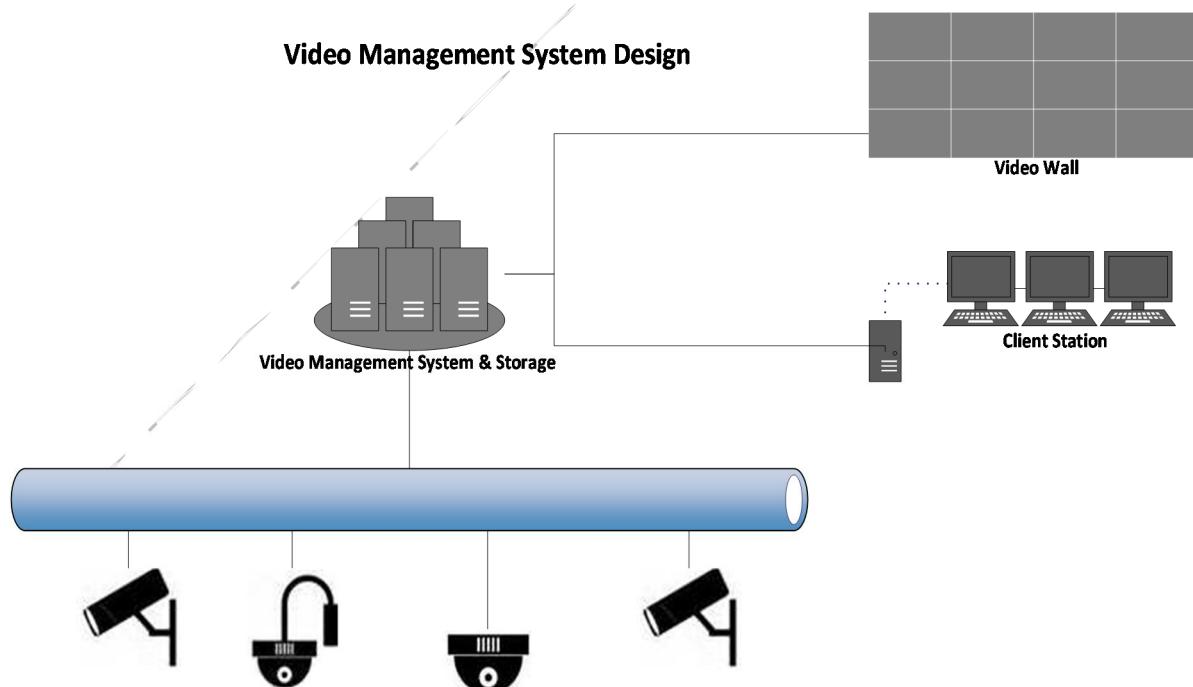
S. No.	Servers	Description
2.	Video Recording Server(s)	The Video Recorder Server shall be a dedicated server that shall store and processes video with the help of Video Management System
3.	Video Analytics Server (s)	Video Analytics Software shall be installed in the Video Analytics Server, to analyse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

### 6.2.3 General Functional Requirements

- I. All cameras supplied shall be for outdoor 24 X 7 operation with day and night operation with 4 year defect and damage replacement warranty
- II. All cameras shall be installed with
  - a. Pole erection as per standards to provide safety for mounted equipment
  - b. Electrical and Network wiring in conduits protected from environment, pests or other elements
  - c. Earth protection for poles and equipment
  - d. Environment protection rating as per standards for all equipment as per outdoor conditions in Amritsar
  - e. Mounting of all equipment shall meet weight and wind shear protection guidelines
  - f. Bird and pest protection measures for complete installation
  - g. External IR illuminators with range up to 100 meters
  - h. Tamper protection measures
  - i. Surge protection measures
  - j. Theft protection measures
  - k. Replacement of equipment damaged due to any of the above listed causes shall be in scope of the bidder
- III. All cameras shall support H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG technology to reduce bandwidth and storage requirements of the system.

- IV. All video feeds shall be either directly encrypted or carried through encrypted tunnel using AES 256, TLS 1.2/PKI, FIPS 140-2 grade protection or equivalent high grade end to end encryption technology.
- V. The cameras shall support only secure PKI certificate based authentication mechanism for both ONVIF and web based administrative access for the cameras. The certificate authority shall be secured using best in class technology in case of self-signed certificates.
- VI. All mounting , field of view and focal length adjustment for cameras shall be done in discussion with police department based on local surveillance requirements
- VII. All cameras shall support minimum 3 streams with configurable resolution, framerate and compression that can be directed to any IP/URL address. It shall be possible to configure these streams for connectivity to ICCC Data Centre, Disaster Recovery Site (at a later date) and local police stations/LPU's etc.
- VIII. Amritsar Police may review requirements for video resolution, FPS and may change these numbers to suit certain specific requirements at any given point.
- IX. It system shall allow SMS and EMAIL alerts to be sent to any concerned person for escalation of a situation under a Standard Operating Procedure (SOP).
- X. Housing of box camera and glass shall be certified by camera OEM or from the same camera OEM for optimal performance of the camera.
- XI. The MSI shall leverage GPU based processing for video analytics wherever possible to reduce the video analytics hardware server requirements and processing time.

#### 6.2.4 Video Management & Recording System



The Video Management System (VMS) can bring together physical security infrastructure over the IP network as the platform for managing the entire surveillance system using high end security with encryption for video in motion and rest.

- I. The IP Cameras (Fixed & PTZ) installed in the identified locations shall be transmit encrypted video feeds to ICCC VMS & Recording Servers for viewing a CCC for police through Junction Boxes with industrial grade network switches that connect to leased backhaul network from ISP's.
- II. The VMS shall support Open standards which are scalable, can integrate Cameras from different manufacturers and provide the ease of integrating with other third party applications in the future.
- III. The VMS shall provide a Server - Client architecture and multiple client viewing options using multicasting techniques based on the solution architecture of the MSI.
- IV. The VMS shall be scalable system that shall permit the retrieval of live or recorded video anywhere, anytime on a variety of clients and also through a web browser interface after proper authentication.
- V. The cameras and surveillance system shall support Maximum Full HD (1920X 1080) resolution at 30 FPS (across all channelsstreams).
- VI. The cameras and surveillance system shall support 30 frames per second (across all channels)
- VII. The cameras and surveillance system shall support Adjustable resolution, quality, and frame rate settings:
  - a. Adjustable by camera
  - b. Adjustable by time schedule
- VIII. The cameras and surveillance system shall support Alarm and other event-triggered recording available
  - a. Adjustable by frame rate, resolution and quality on alarm
- IX. The cameras and surveillance system shall support Continuous Recording
  - a. Adjustable by camera
  - b. Adjustable by schedule
- X. The cameras and surveillance system shall support Motion-based Video Recording
- XI. The cameras and surveillance system shall support advanced compression methods available ("H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG" etc.) on all existing and new cameras installed.
- XII. The surveillance system shall support intelligent storage methods
  - a. Ability to store evidence for period of 30 days with automatic overwriting
  - b. Ability to adjust storage duration
  - c. Ability to store images by event type (e.g. ANPR alert, Face Recognition alert, motion-based, alarm-based etc.)
  - d. Ability to adjust storage duration by event type
  - e. Ability to retain important evidence for longer duration based on flagging by police personnel
  - f. The system shall use NL-SAS drives for storing video
  - g. Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data.
  - h. It shall be possible to view archived video online without need for downloading it
  - i. The system shall perform automatic archival to tape library without user intervention on regular-interval and/or storage size basis
- XIII. The surveillance system shall support RAID storage to prevent data loss

- a. RAID offered as an upgrade or standard feature
- XIV. The surveillance system shall support Analogue and IP camera from multiple makes and their models i.e. Fixed Box, Dome, PTZ, Panoramic etc. The surveillance system shall support PTZ protocols of all existing and new cameras being installed.
- XV. User interface and functionality shall be consistent across support of all the different types of cameras supported
- XVI. The surveillance system shall support multiple camera API's
- a. Ability to easily integrate new camera technologies and/or functionalities through a camera API
  - b. Camera API enables user interface and functionality to be consistent across support of all the different types of cameras supported
- XVII. The surveillance system shall support channel expansion on the same license at additional per channel cost. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
- XVIII. The surveillance system shall support Multi-camera viewing on large video walls
- a. Multiple cameras displayed in single video wall screen
  - b. 14.2 The system shall support digital zooming on live and recorded video
  - c. 14.3 Browsing recordings from storage systems
  - d. 14.4 Creating and switching between multiple of views.
  - e. 14.5 Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
  - f. 14.6 Controlling PTZ cameras.
  - g. 14.7 Using sound notifications for attracting attention to detected motion or events.
  - h. 14.8 Getting quick overview of sequences with detected motion.
  - i. 14.9 Getting quick overviews of detected alerts or events.
  - j. 14.10 Quickly searching selected areas of video recording for motion (also known as Smart Search).
- XIX. The surveillance system shall support Virtual matrix
- XX. The surveillance system shall support simultaneous recording, live viewing, and remote transmission
- XXI. The surveillance system shall support live video monitoring application
- a. Sequencer and multi-camera viewing shall be available on the software
  - b. Alerting capabilities on the live video feed
- XXII. The surveillance system shall support surveillance activity summary display
- XXIII. The surveillance system shall support adjustable image sizes for enlarged viewing
- XXIV. The surveillance system shall support ability to create and name camera groups
- XXV. The surveillance system shall support Event naming
- a. Open naming fields and canned pick lists
- XXVI. The surveillance system shall support ability to create alerts
- a. For activity in restricted zones (defined by motion grid)
  - b. For activity at restricted times
  - c. Send alerts including thumbnails via email, SMS and VOIP call
- XXVII. Ability to conduct correlated searches (e.g. all motion occurring within 2 minutes of "event id")
- XXVIII. Thumbnail image display of search results

- XXIX. Ability to search by specific data fields
- XXX. Ability to search for events across systems
- XXXI. Ability to search and review face images
- XXXII. Ability to search a specific face by similarity
  - a. Across systems and locations
- XXXIII. Ability to search activity within a specific region
- XXXIV. Ability to search by direction of motion
- XXXV. The system shall support saving searches
- XXXVI. Cases stored and managed centrally
- XXXVII. Case management and investigation tools can be accessed from a single application by multiple investigators simultaneously.
- XXXVIII. Case exporting
  - a. Export to PC, CD, or email
  - b. Video player included with case or files in a universal format that does not required proprietary video player
  - c. Case export in a format that is easily viewable (e.g. HTML and XML) and able to import into other systems for reporting or analysis.
- XXXIX. The system shall support Video/image retrieval
  - a. 36.1. Ability to specify types of events shown in real-time
- XL. Ability to import images, and search against imported images
- XLI. Ability to verify authenticity of video and events through watermarking method (e.g. Secure Hash Algorithm). It shall be possible to watermark camera location, date, time, Frame Rate, Resolution etc.
- XLII. The surveillance system shall support Time/Date, Camera Location, Frame Rate, and Resolution Overlay on video/images. All devices shall be synchronized with NTP server for date and time.
- XLIII. Ability to add analytics as software upgrades without require buying additional hardware
- XLIV. The surveillance system shall support edge analytics on cameras
- XLV. The surveillance system shall support complete integration with Facial Recognition and Automatic Number Plate recognition software.
- XLVI. The surveillance system shall support Directional Motion Analysis
- XLVII. The surveillance system shall support Regional Motion Analysis
- XLVIII. The surveillance system shall support Object added/removed Analysis
- XLIX. The surveillance system shall support License Plate Recognition
  - L. The surveillance system shall support Analytics-triggered alerts
  - LI. The surveillance system shall support Search by analytics (outside of alerts) (e.g. search in a region, or search for a specific person where no alert has been set)
  - LII. The surveillance system shall support People analytics like Dwell Time, Loitering, People Counting, Queue Length and Crowd Detection.
- LIII. API to integrate data from external, non-video system such as transaction, POS, and access control etc.
  - a. Web standard protocol (e.g. REST/SOAP)
  - b. Supported integration methods (e.g. IP, serial)
  - c. It shall be possible to integrate the system to Social Media and Citizen Engagement software for monitoring incidents or crime

- LIV. Integration with DVR/NVR's UI and Functionality
  - a. Integrated data events have same functionality as other surveillance activity in system (e.g. date/time/camera/system searching, correlated searching).
  - b. Data events seamlessly integrated into UI
  - c. Data events fields customizable
  - d. Data events stored centrally
  - e. Data events can be stored separately and longer than video
  - f. Ability to search by specific fields and details (e.g. account #, sequence #, transaction type, or other fields)
- LV. API to integrate 3rd party software analytics and/or hardware into DVR/NVR or support remote analysis hardware
  - a. Web standard protocol (e.g. SOAP)
- LVI. Integration with DVR/NVR's UI and Functionalities
  - a. Integrated data events have same functionality as other surveillance activity in system (e.g. date/time/camera/system searching, correlated searching).
  - b. Data events seamlessly integrated into UI
  - c. Data events fields customizable
  - d. Data events stored centrally
  - e. Data events can be stored separately and longer than video
- LVII. Ability for 3rd parties receive data from DVR/NVR according to specified criteria
  - a. Use of standard web protocols (e.g. RSS)
  - b. System events are encoded in format for easy parsing, transformation, or rendering (e.g. XML)
  - c. Customize feeds for any set of data and also alerts
- LVIII. Enterprise management of systems (i.e. single sign on ability to manage distributed systems centrally)
- LIX. Remote configuration of systems
  - a. Ability to adjust all types of recording settings (such as resolution, quality, fps, motion-based or continuous recording) remotely. This should be possible on 100% of the cameras to conserve bandwidth and storage.
  - b. Ability to adjust global camera settings remotely (e.g. frame rates across all cameras)
  - c. Ability to adjust individual camera settings remotely
  - d. Ability to configure storage settings (such as RAID configurations) remotely
- LX. Ability to upgrade "over the wire" for easier hardware and software updates
- LXI. Saved configurations in case of system failure
  - a. Automatic backup of individual appliance configurations, enabling quick restoration of settings on a replacement box.
  - b. Number of past configuration versions saved
- LXII. Saved system and camera templates available, which can be applied to systems/sites and cameras
- LXIII. Remote troubleshooting
  - a. Remote reboot available
  - b. Live video check available
  - c. Testing connectivity of servers available
- LXIV. NTP Time Synchronization
- LXV. Ability to centrally manage users and roles across sites/systems

LXVI. Ability to remotely manage users and roles

LXVII. Ability to create users

- Ability to grant access to specific regions and/or systems
- Ability to assign roles with specific permissions (e.g. creating an investigator role, which allows one with an investigator role to edit cases but not configure system settings)
- Ability to enable automatic password expiration
- Ability to enable automatic password renewal

LXVIII. Remote health monitoring

LXIX. Enterprise health monitoring

LXX. Health alerts available

- Cameras health alerts
- Camera or camera connection failure
- Camera added or removed
- Network connection failure
- System not recording
- Software update needed
- External data not received (e.g. data from transaction system not received)
- Email alerts customizable by type of alert and recipient
- Intelligent filtering of nuisance alerts
- The system shall support SNMP alerts for integration with third party systems

LXXI. Reporting

- Ability to view summary of health alerts
- Ability to run customized report of system issues
- Ability to create and run customized summary of systems' health (to meet end-user's security standards) including system and channel configurations and transaction events being received.

LXXII. Audit

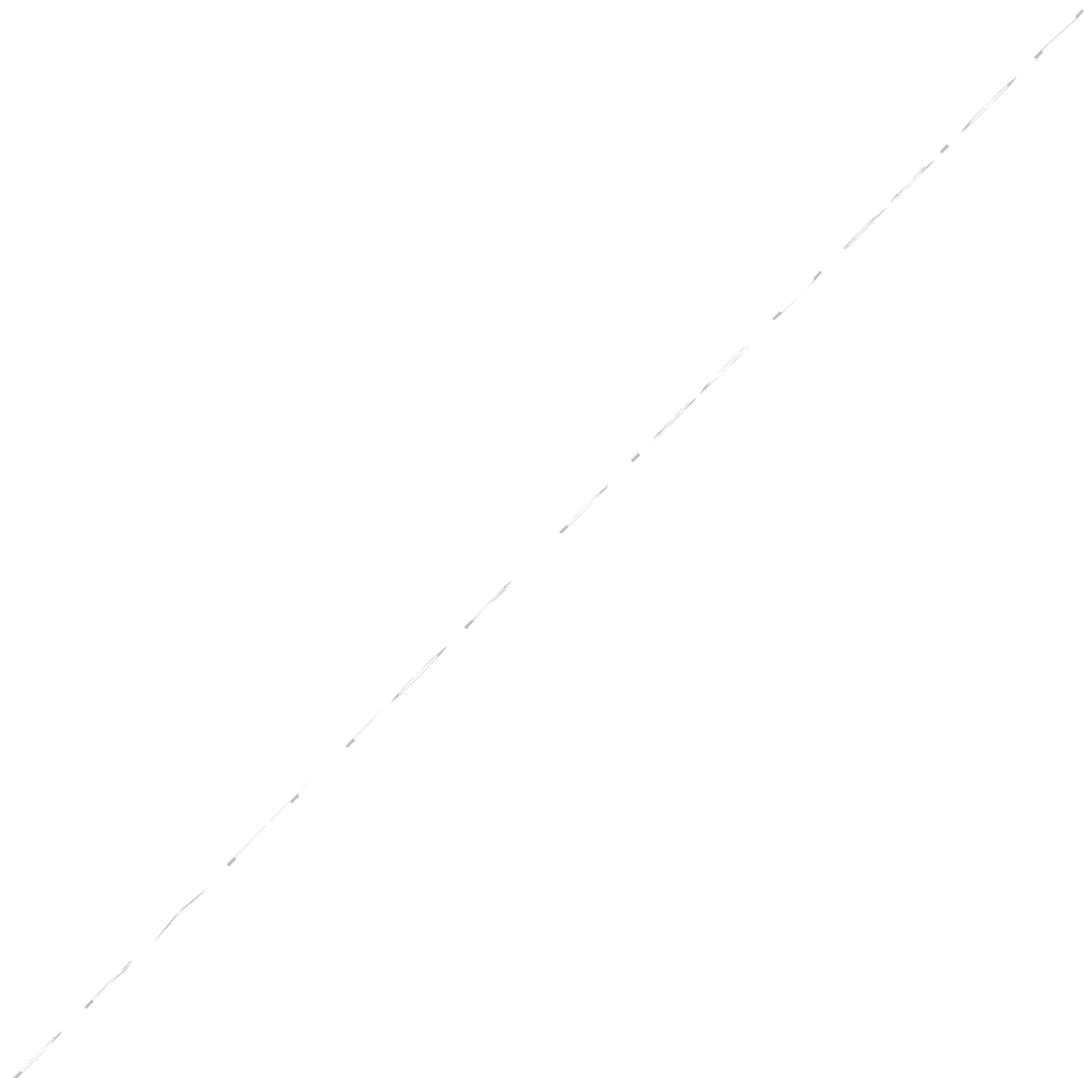
- The system shall support keeping record of all administrative actions for audit purpose
- The system shall support keeping record all system logs, event logs, alert logs and audit logs

LXXIII. Resiliency

- The surveillance system shall continue to record video from surveillance cameras on recording servers irrespective of availability of video management or other servers irrespective of it being offline
- The video recording servers shall support automatic failover to multiple failover servers for a group of recording servers. This functionality shall be accomplished by failover server as a standby unit that shall take over in the event that one of a group of designated recording servers fails. Recordings shall be synchronized back to the original recording server once it is back online.
- The video management server and database shall support automatic failover to a failover server.

- LXXIV. The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
- LXXV. The system shall support the rules based event/actions such as Starting and Stopping recording , Set non-default live frame rate, Set non-default recording rate ,Start and stop PTZ patrolling, Send notifications via email , Pop-up video on designated Client Monitor recipients etc.
- LXXVI. The Video Recorder Server will be a dedicated server that will store and processes video with the help of Video Management System.
- LXXVII. The system should be capable of continuous video recording for period of 30 days.
- LXXVIII. The system shall automatically overwrite the data after 30 days. It should be noted that at any point of time the local storage at the storage servers should have the data of previous 30 days. Direct extraction through any physical device like USB flash drive, Portable Hard disk etc. shall be possible
- LXXIX. The surveillance solution shall support web and mobile viewing of live video feeds after multi-factor authentication mechanisms over secure and encrypted interfaces. Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication. Amritsar Police may provide such tablets / smart phones to the designated Police Personnel. It shall be responsibility of MSI to configure such tablets / Smartphone, for the Surveillance System being implemented a part of this project, and ensure that all the necessary access is given to these mobile users. Functionalities to be provided through mobile application: Viewing of any video stream from Central VMS, uploading of video / pictures central VMS, Location based GIS Map access, tagging of mobile device/location information for all relevant functionalities.
- LXXX. All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts, privacy laws, cybersecurity laws and other applicable government laws and regulations in India.
- LXXXI. System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and MSI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose & the same can be listed in miscellaneous section of the commercial bid. MSI shall also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.
- LXXXII. Any hardware or software required to achieve the functional requirement and technical solution of the overall Project (may not be not specified in the schedule) is to be proposed in the Bid and the applicable cost shall be borne by the MSI.

LXXXIII. There would be the provision for Third party audit periodically, paid by ASCL separately. ASCL reserves the right to appoint any Independent Evaluation Agency at any time during the phases of the project.



### 6.2.5 Video Analytics

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

Below table provide indicative break-up of camera locations with type of analytics and camera count at those locations types:

S. No	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
1.	All Locations Fixed Cameras + PTZ + ANPR	<ul style="list-style-type: none"> <li>· Video Recording</li> <li>· Camera Blocked</li> <li>· Camera Dusty</li> <li>· Camera Focus</li> <li>· Camera FOV Change</li> <li>· Privacy Protection</li> </ul>	21	35	75	778	130	72
2.	All Locations PTZ Cameras	<ul style="list-style-type: none"> <li>· Automatic object/person recognition and tracking with PTZ cameras</li> <li>· Alarm object tracking from fix camera to PTZ camera</li> <li>· Alarm object tracking from PTZ camera to PTZ camera</li> <li>· Object tracking underneath the camera</li> </ul>	0	0	0	0	130	0
3.	Crime Hotspots	<ul style="list-style-type: none"> <li>· Face Recognition</li> <li>· ANPR</li> <li>· Un-attended object origin search</li> </ul>	7	29	0	8	7	15

S. No	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
		<ul style="list-style-type: none"> <li>Person of Interest Origin Search</li> <li>Loitering</li> </ul>						
4.	Procession/Protest Hotspots	<ul style="list-style-type: none"> <li>Crowd Detection in Area of interest</li> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	20	10	0
5.	Traffic Congestion Stretch	<ul style="list-style-type: none"> <li>Traffic Congestion Detection (by Avg Speed)</li> <li>Wrong Direction Traffic Flow</li> </ul>	0	0	0	10	8	0
6.	City Entry/Exit Points	<ul style="list-style-type: none"> <li>ANPR</li> </ul>	0	0	0	0	0	42
7.	Railway Stations Entry/Exit Points	<ul style="list-style-type: none"> <li>Face recognition=4</li> <li>ANPR</li> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	4	0	0	0	0	4
8.	Bus Stations Entry/Exit Points	<ul style="list-style-type: none"> <li>Face recognition</li> <li>ANPR</li> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	10	0	0	4	4	6

S. No	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
9.	Airport Entry / Exit Points	<ul style="list-style-type: none"> <li>Face recognition</li> <li>ANPR</li> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	3	1	4
10.	Tourist Hotspots Entry/Exit Points	<ul style="list-style-type: none"> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	12	0	0
11.	Main Markets Entry/Exit Points / Prime view	<ul style="list-style-type: none"> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	10	9	0
12.	Schools	<ul style="list-style-type: none"> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	9	0	0
13.	Government Colleges (Entry/Exit Points)	<ul style="list-style-type: none"> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	9	0	0
14.	Government Hospitals	<ul style="list-style-type: none"> <li>Un-attended object origin search</li> <li>Person of Interest Origin Search</li> </ul>	0	0	0	8	1	0
15.	Traffic Junctions	<ul style="list-style-type: none"> <li>Congestion Detection</li> <li>Wrong way driving</li> </ul>	0	0	0	6	6	

S. No	Location Type	Video Analytics Type at Locations	Indoor Face (Bullet)	Outdoor Face (Fixed Box)	Panoramic 360° Camera	Surveillance (Fixed Box)	PTZ Camera	ANPR (Fixed Box)
16.	Parking Lots	- ANPR	0	0	0	0	0	4
17.	Administrative Building	- Motion Detection Indoor/Outdoor Trip Wire	0	0	0	8	0	0

## Functional Requirement of Video Analytics

S. No.	Nature of Requirement	Minimum Requirement Specifications
VCA-FR-01	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
VCA-FR-02	General Requirements	The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.
VCA-FR-03	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
VCA-FR-04	General Requirements	The system shall allow the configuration of applicable rules and manage them.
VCA-FR-05	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size.
VCA-FR-06	General Requirements	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event
VCA-FR-07	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene
VCA-FR-08	General Requirements	The system shall enable detecting rules in the defined areas (zones/ lines)
VCA-FR-09	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.
VCA-FR-10	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately
VCA-FR-11	General Requirements	The system shall allow classification of different objects like animals, vehicles, people etc.
VCA-FR-12	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.
VCA-FR-13	General Requirements	VCA shall provide secured feeds with encryption, watermarking for data authenticity
VCA-FR-14	General Requirements	VCA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.
VCA-FR-15	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system
VCA-FR-16	General Requirements	VAS should allow to add, edit, delete or disable and enable Policies.
VCA-FR-17	Features	The city wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms

S. No.	Nature of Requirement	Minimum Requirement Specifications
		& triggers. The solution should offer following triggers from Day1:
VCA-FR-18	Security Features	Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA), Unattended object, Object Classification, Tripwire / Intrusion, Loitering, etc.
VCA-FR-19	Traffic / Parking Features	Vehicle Wrong Way Detection, Illegal Parking Detection, Congestion Detection, Vehicle Counting, Speeding Detection, Parking Management etc.
VCA-FR-20	Enhanced Monitoring Features	Video Stitching with Object Tracking, Video Stabilization, Video Smoke Detection, Video Fire Detection etc.
VCA-FR-21	Crowd Management	Crowd Control, Counter-Flow Detection, People Counting, Line Control, People Tracking etc.
VCA-FR-22	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)
VCA-FR-23	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification,
VCA-FR-24	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.
VCA-FR-25	General Requirements	The system shall allow classification of different objects like animals, vehicles, people etc.
VCA-FR-26	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events such as motion Detection etc. as picked up by Camera without the need for human intervention
VCA-FR-27	General Requirements	VCA shall provide secured feeds with encryption, watermarking for data authenticity
VCA-FR-28	General Requirements	VCA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.
VCA-FR-29	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system
VCA-FR-30	General Requirements	VAS should allow to add, edit, delete or disable and enable Policies
VCA-FR-31	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence
VCA-FR-32	General Requirements	The system shall provide configurable detection zones and lines to detect events of interest, Detection

S. No.	Nature of Requirement	Minimum Requirement Specifications
		zones define an area of interest and Detection lines define a perimeter instead of a region.
VCA-FR-33	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
VCA-FR-34	General Requirements	The system shall allow the configuration of applicable rules and manage them.
VCA-FR-35	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size
VCA-FR-36	General Requirements	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event
VCA-FR-37	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene
VCA-FR-38	General Requirements	The system shall enable detecting rules in the defined areas (zones/ lines)
VCA-FR-39	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.
VCA-FR-40	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately
VCA-FR-41	Features	<p>The city wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms &amp; triggers. The solution should offer following triggers from Day1:</p> <ul style="list-style-type: none"> <li>a. Parking Violation</li> <li>b. Wrong Direction</li> <li>c. People loitering</li> <li>d. Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA)</li> <li>e. Unattended Object</li> <li>f. Crowd detection</li> <li>g. Traffic flow/Congestion</li> <li>h. Traffic Volume estimation and statistical counts</li> <li>i. People tracking</li> </ul>
VCA-FR-42	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)
VCA-FR-43	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification

S. No.	Nature of Requirement	Minimum Requirement Specifications
VCA-FR-44	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.

The analytics system shall help in resolving the following use cases:

S. No.	Nature of Requirement	Detailed use case
1.	Camera Tampering	Alert to be generated when camera has been tampered by way of change of Field of view of camera, blurring of view, blocking of view by cloth or obstruction, camera disconnection, blinding of camera by laser or flashlights
		Once alert is generated, the incident should be flagged and system should have the capability to trace the person responsible for the sabotage in other cameras and send notification to nearest Police asset on the field about the person of interest. The track/trace of the person shall be shown on the map.
2.	Crowd Monitoring and Detection	Inside the city, when crowd monitoring is done at sensitive locations, and if crowd reaches above certain threshold, alarm should be created in the control room.
		During processions etc. as the crowd starts gathering and reaches certain level, these cameras should automatically popup along with alarm and start monitoring from CCC by dragging these cameras on video wall
3.	Abandoned/Unattended Object detection and Person/Object Origin Search	Alert for the Object detected in an area of interest that has been left more than specified time span
		The system shall be able to track the person who left the object across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map. It shall be possible to search both known and unknown faces in the system within network of cameras in the area.
4.	Perimeter Protection	Detection of intruder entering/exiting a given area of interest
		Once verified and confirmed by operator that it is a rogue person, the system shall be able to track the person across various cameras and to find the origin of such person. The track/trace of the person shall be shown on the map
5.	Person tracking over network of cameras	Tracking of person based on image captured from the proposed IP camera footage, e.g. pause the video and track the person of interest in multiple IP cameras and stored video footage of 30 days
		Tracking of person based on verbal clues given to the central control room e.g., man having beard, dark skin, with white

S. No.	Nature of Requirement	Detailed use case
		shirt and blue jeans and black jacket. The system shall trigger search and tracking based on attribute based search Tracking of people based on Full body photographs received by the police control room Tracking and detection of people based on Facebook or social media profiles on camera footage as well as recorded video footage
6.	Person Tracking - Combination of Face Recognition Cameras and person of interest tracking capability	Track a specific person identified by the Face Recognition cameras. The Face Recognition devices must be able to provide the full frame of the person for enhanced tracking The person of interest search application shall allow access to all relevant associated VMS recordings to track the person of interest in multiple IP cameras

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

- I. Auto Tracker: To detect and track movement in the field of view.
- II. Adaptive Motion Detection: To detect and track object that enter a scene and then triggers an alarm when the object enter a user-defined zone.
- III. Abandoned Object: To detect objects placed within a defined zone and triggers an alarm if the object remains in the zone longer than the user-defined time allows.
- IV. Camera Sabotage: Triggers an alarm if the lens is obstructed by spray paint, a cloth or a lens cap.
- V. Directional Motion: Generates an alarm in a high traffic area when a person or object moves in a specified direction.
- VI. Object Removal: To triggers an alarm if the object is removed from a user-defined zone.
- VII. Stopped Vehicle: To detect vehicles stopped near a sensitive area longer than the user-defined time allows.
- VIII. Intrusion Detection - Detect intrusion

#### 6.2.5.1 Face Recognition System (FRS)

- I. Face Recognition cameras shall be Full HD (1920 X 1080) @ 30 FPS and shall be installed at transit hubs like Airports, Railway Stations and Bus Stands at building entry and exit gates (indoor environment). These shall also be installed at crime hotspots in the city in an outdoor environment
- II. These cameras shall be mounted at a height of approximately 5-10 feet to capture faces clearly at distance of up to 3 meters
- III. The face recognition cameras shall transmit maximum resolution uncompressed video feed for best face recognition results to Local Processing Unit (LPU) inside junction boxes for processing and extracting face recognition minutiae from the

- video feed. Only minutiae shall be shared with Face Recognition head end software at the ICCC for further matching and alert generation Alternatively, video streams can also be analysed at server end without local processing unit
- IV. The face recognition cameras shall send a compressed video stream to ICCC for video recording and analytics for evidence purpose and general surveillance
  - V. The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system
  - VI. The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the System Integrator
  - VII. The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real time report such as Audit log report, Hit List Report, Daily Statistics Report, and Distribution Report
  - VIII. The facial recognition system should be accessible from 5 different desktop/laptops at any given time. When choosing a distributed architecture, the system shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision
  - IX. The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts
  - X. The algorithm for facial recognition or the forensic tool should be able to recognize partial faces with varying angles
  - XI. The system should be able to detect multiple faces from live single video feed
  - XII. The system should have combination of eye-zone extraction and facial recognition
  - XIII. The system should have short processing time and high recognition rate
  - XIV. The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)
  - XV. Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc. The FRS system shall use of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments
  - XVI. The system should be able to identify and authenticate based on individual facial features
  - XVII. The system should be compatible with the video management system being proposed by the system integrator
  - XVIII. The system should have capability for 1:1 verification and 1: N identification matching
  - XIX. The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.

- XX. The system should be able to support diverse industry standard graphic and video formats as well as live cameras
- XXI. The system should be able to match faces from recorded media
- XXII. The system should be able to detect a face from a group photo
- XXIII. The system should be able to detect a face from stored videos of any format
- XXIV. The system should have bulk process of adding faces in the system
- XXV. The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing
- XXVI. The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for windows OS or android OS to capture a face on the field and get the matching result from the backend server
- XXVII. The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas
- XXVIII. The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted"
- XXIX. It should be able to provide information such as Gender & Age Group along with facial detection/match data
- XXX. The face recognition algorithm used in the facial recognition system shall be among the top 5 vendors in the latest Face Recognition Vendor Test (FRVT) report from NIST as on date of publish of this DPR

Face Recognition System (FRS) is designed for identifying or verifying a person from various kinds of photo inputs from digital image file to video source. The system should offer logical algorithms and user-friendly, simple graphical user interface making it easy to perform the facial matching.

The system can be able to broadly match a suspect/criminal photograph with database created using photograph images available with Passport, CCTNS, and Prisons, State or National Automated Fingerprint Identification System or any other image database available with police/ other agencies

The system can be able to:

- I. Capture face images from IP Camera feed and generate alerts if a blacklist match is found.
- II. Search photographs from the database matching suspect features
- III. Matching suspected criminal face from pre-recorded video feeds obtained from IP cameras deployed in various critical identified locations, or with the video feeds received from private or other public organization's video feeds
- IV. Adding photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches
- V. Investigate to check the identity of individuals upon receiving such requests from Police Stations

### 6.2.5.2 Automatic Number Plate Recognition (ANPR)

The ANPR System shall have the following in built features:

- I. The ANPR System should be capable of detecting and converting vehicle license plates into English readable OCR data. The system should support real-time detection of vehicles at the deployed locations, recording each four wheelers, 2 wheelers and other vehicle type number plate, database lookup from central server and triggering of alarms/alerts based on the vehicle status and category as specified by the database. The system usage should be privilege driven using password authentication for VMS GUI access
- II. ANPR cameras shall be mounted at City Entry/Exit Points and at Transit Hubs like Railway Stations, Bus stands and Airports primarily for purpose of surveillance only. The system shall have capability to compare license plates against a blacklisted or stolen vehicle database that is part of the system for alert generation
- III. It shall be possible to get all real-time alerts on a city map at ICCC, related to location of detection of blacklisted vehicle with all extracted data characteristics of the vehicle including speed
- IV. The system shall also show location of all existing Dispatch Units on a map to know which one is closest to the location
- V. The system shall have capability to integrate with an external Computer Aided Dispatch (CAD) system via API and the MSI shall be responsible to make this integration to trigger automatic incident creation and dispatch on detection of the blacklisted vehicles
- VI. The system shall have capability to queue all pending incidents (of detection of blacklisted vehicles) so that CAD operators can attend to them one by one.
- VII. The system shall maintain complete record of all vehicles detected in an audit trail for record keeping and audit purpose
- VIII. ANPR cameras shall be required to work at 30 FPS at Full HD (1920 X 1080) resolution with 5 to 50 mm lens high quality lens.
- IX. The ANPR cameras can transmit uncompressed video feeds for better accuracy to Local Processing Units (LPU) inside the junction boxes for extracting
  - a. Vehicle Number Plate
  - b. Other characteristics like vehicle colour, type, count etc. using Automatics Traffic Counter Classifier (ATCC) function
  - c. Speed of the vehicle
- X. A single compressed stream shall also be sent to server for recording and general video analytics purpose
- XI. The LPU shall transfer the extracted metadata with cropped license plate images to the ANPR head end software for further processing and alerts generation.
- XII. At the City Entry/Exit points they shall be required to be mounted on a cantilever pole arm with each ANPR camera covering one lane. The height of installation shall be approximately 6 meters
- XIII. At the transit hub they shall be mounted at entry and exit gates and installed to cover all vehicles that enter and exit these locations
- XIV. Vehicle Detection and Video Capture Module

- a. The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition.

#### XV. License Plate Detection

- a. The System shall automatically detect the license plate in the captured video feed in real-time.
- b. The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts).
- c. The System shall store JPEG image of vehicle and license plate and enter the license plate number into database along with date time stamp and site location details.
- d. System should be able to detect and recognize the English alpha numeric License plate in standard fonts and formats of all vehicles including cars, HCV, and LCV.
- e. The system should be able to process and read number plates of vehicles with speed of up to 200 km/hr.
- f. The system shall be robust to variation in License Plates in terms of font, size, contrast and color and should work with good accuracy.

#### XVI. Colour Detection

- a. The system shall detect the color of all vehicles in the camera view during daytime and label them as per the predefined list of configured system colors. The system shall store the color information of each vehicle along with the license plate information for each transaction in the database
- b. The system shall have options to search historical records for post event analysis by the vehicle color or the vehicle color with license plate and date time combinations

#### XVII. Alert Generation

- a. The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel
- b. The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories

#### XVIII. Vehicle Log

- a. The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.
- b. The system should provide advanced and smart searching facility of License Plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1 and 2 character distance)

#### XIX. Vehicle Make Detection Module

- a. System should be able to identify the make of the vehicle coming in the field of view of the camera with good accuracy

XX. Vehicle Classification module

- a. System should be able to classify the vehicle into LMV, HMV and 2-wheelers

XXI. Over Speed Detection Module:

- a. The system should be able to detect vehicles moving up to speeds of 200 km/hr and read their number plates with good accuracy. Vendor should provide manufacturer certificate/test report in support of their claim
- b. The certification for the accuracy of speed measurement should be from the approved Govt. body from the country of origin. Certifications shall be provided for the complete system and not individual components. The system should be calibrated for accuracy prior to handing over and the successful bidder should ensure annual calibration of the system

XXII. Central Management

- a. The Central Management Module shall run on the ANPRS Central Server at ICCC. It should be possible to view records and edit hotlists from the Central Server

XXIII. The system should be able to do - No helmet detection for 2-wheelers

XXIV. The system should have reading accuracy of 80% on vehicles including 2 & 4 wheelers which are visible by human eye for English alphanumeric number plates excluding cursive fonts

#### [6.2.5.3 Crowd Detection and People Counting in Camera View](#)

Crowd monitoring and activities understanding using visual methods is significant in many surveillance applications. Crowd density evaluation is one of the most fascinating nuisances in crowd analysis. A common application on crowd density evaluation is automatic monitoring of the crowd density in communal places for security control such as crowd congestion detection and evacuation detection. Most methods proposed in the literature can be categorized into two types: direct and indirect approaches. Direct approach is a detection based method that detects each individual person in a scene using segmentation or human detection.

The total number of persons can then be determined easily. Some of these methods involve explicit detection, tracking, and monitoring of individuals in the scene such as the use of histogram of oriented gradients (HOG) features for person and the indirect approach is a map based approach that maps some detected visual features to the number of people. Crowd movement tracking is quite altered from tracking individuals in the crowd

- I. Provides flexibility in installation. It can be installed either in the same machine as VMS or in a separate machine
- II. Can take video feed directly either from camera or VMS
- III. Can send alarms to VMS viewer (like smart client) applications
- IV. Can run as a windows service up to 100 channels per server

- V. Supports Failover
- VI. Supports ONVIF to get video stream from camera and send video stream to VMS
- VII. Supports several leading VMS

#### 6.2.5.4 Privacy Masking

For a smart and safe city, the safety and security aspects cannot be compromised. Video Surveillance and Automated Monitoring through Video Analytics are as inevitable for critical zones and high-security areas as they are for general public places. Be it School & Colleges, or even Airports or Malls, you need to put up a full-proof security monitoring system in place. The trade-off is infringement of people's privacy. The challenge, therefore, is to monitor the places while ensuring the privacy need for people under surveillance.

- I. Run privacy masking in real-time for the video shown live to monitoring personnel
- II. Simultaneously record & store unmasked video for back up and future reference
- III. Option to run the privacy masking on any previously recorded video as well
- IV. Configure masking once it works for all video frames and all agents in the video
- V. Selective masking can be done for a specific area as against the complete screen
- VI. Effective even in continuous crowd where it can ensure privacy for all the faces
- VII. Supports privacy masking for people of any ethnicity & complexion
- VIII. Inbuilt models and custom models take care of different illumination levels during day/night time

#### 6.2.5.5 Un-Attended Objects

The left out object detection application automatically identifies any foreign physical object for example bags, boxes or any inanimate objects kept/left un-attended in the user defined region of interest in the field of view of a surveillance camera and automatically generates alerts with relevant information for subsequent processing by a system or an operator.

To achieve maximum accuracy of this application, following are basic requirements:

- I. The field of view should be "uniformly" illuminated
- II. Captured video from camera should be of high quality. There should not be any flickering, visible noise, motion blur in the captured video from the camera for desired accuracy
- III. Network bandwidth should be stable and non-fluctuating for smooth video and no loss of frames
- IV. The network should have enough bandwidth to capture video with highest quality and highest bitrate allowed in the camera for best accuracy
- V. The camera "FPS" (frames per second) must be stable and non-fluctuating
- VI. The camera should be installed in a stable platform so that there is no vibration of the camera.
- VII. Camera view should not be tilted
- VIII. Avoid region with glare, glass walls, flashing lights, trees etc.
- IX. Camera should be focused for very sharp imagery
- X. Height of the camera from the floor should be at least 7ft up and camera down angle

XI. Should be maintained to make any object (human/vehicle) present in the scene, fully visible throughout the movement

#### 6.2.5.6 Vehicle Count

Video Based Automatic Traffic Counting & Classification for National Highway applications using IP Cameras and intelligent counting units, the Video Turnstile vehicle traffic counting system achieves over 98% accuracy in all conditions: day and night in rain, sun and snow.

One can set the vehicle traffic detectors to count vehicles going straight on or turning. One camera can cover several exits of a junction. At four-way junctions, for example, the system provides multi-directional counts for vehicles turning north, south, east or west and coming from any direction.

The system is designed so that

- I. Traffic data is uploaded securely in real-time to web browsers: users can log into their password-protected on-line accounts from anywhere
- II. There is no limit to the number of roads and junctions on which traffic can be counted using the scalable IP Camera system
- III. Users can easily verify the vehicle counts simply by watching the video back and seeing the counts increase as the cars pass
- IV. Counts can cover any period of time: the number of cars passing in each hour or each day for example
- V. Local video analytics minimises bandwidth use
- VI. It is simple to set up and non-intrusive. No components need to be installed directly into the road surface and users can easily modify the zones through which vehicles are counted, from their office

#### 6.2.5.7 Vehicle Detection and Tracking Techniques

This approach has three steps for detecting the vehicles i.e. 1. Segmentation 2. Training 3. Validation. In first step, it takes some training images from total number of images depending upon number of frames. Then it proceed with the optimization of the segmentation parameters for segmentation and is repeated for training samples that involve multi-resolution segmentation and the spectral difference segmentation and then it transfer to validation part of object accuracy valuation with the training samples. In this model the condition of applicability to high spatial resolution weakly sensed data, and to address the essential for a quantitative, user-supervised method for taking best segmentation parameters. It developed an impartial metric which is the number of training object matched with maximize area matched and is minimizes below and over segmentation for chosen images in objective primitives. There are some object tracking methods in vehicle tracking:

- I. Region-Based Tracking Methods
- II. Contour Tracking Methods
- III. 3D Model-Based Tracking Methods
- IV. Feature-Based Tracking Methods
- V. Colour and Pattern-Based Methods

#### 6.2.5.8 Wrong way driving

It is described the methodology used to detect and validate the vehicles circulating in the wrong way. In each new frame, the optical motion flow is computed and the median of the flow direction for each blocks are calculated. An object is defined as circulating in the wrong direction when the difference between both the direction of the flow in the present frame and the estimated means of the corresponding block learned are larger than  $2.57\sigma$  for the 99% confidence interval.

It is possible, due to the vibration of the surveillance camera pole and noisy motion flow estimation, that a vector or a set of vectors of flow are detected even if there is no real motion on those blocks of the image. Thus, it is necessary to validate all the objects detected in the wrong way before triggering an alarm. Two types of validation were used, namely a temporal validation, to verify if the detected objects make a coherent trajectory, and an appearance-based validation, to check if that object is really a car.

#### 6.2.5.9 Motion Detection Video Analytic

Motion detection can be used to detect unauthorized entry, for example, if a member of staff leaves by an unapproved exit. Specific areas of interest can be defined in a scene and searched automatically through a recording to identify and view any significant motion that occurred during the recording. This is hugely useful when searching for motion in a quiet area throughout a long period of recorded video. It can be tuned using parameters such as object size and sensitivity. A "no-motion" option lets you monitor things that should be moving and alert when motion stops, e.g. School, College, Government building, night time in-front bank and blank places.

#### 6.2.5.10 Perimeter Protection

The standard functionality of this perimeter video surveillance system is to deter and detect potential intruders or unauthorised persons from approaching the perimeter. In doing this, the system provides an alarm from Intelligent Video Analytics (IVA) and associated alarm image and video with metadata describing the location and path of the intruder in the event of a perimeter attack. Our perimeter security surveillance solution can also provide advanced object classification, offering both 3D rule based and cognitive object classification in order to minimise nuisance alarms caused by animals, inanimate objects, vegetation and shadows. Features of our Perimeter Protection System:

- I. Above 99% long range detection accuracy with extremely low false alarm rate
- II. Advanced object classification with 12 pre-defined classes and support for user defined classes
- III. Simple and fast template based configuration
- IV. Deployable as the sole perimeter protection system
- V. Reduce perimeter security surveillance costs through deploying object classification on wide Field of View cameras and therefore cutting down on camera count

- VI. Increase operational efficiency and prevent theft and vandalism
- VII. Flexible deployment model - server or edge based perimeter video surveillance analytics
- VIII. Optional cloud based alarm hosting service

#### 6.2.5.11 Congestion Detection

Proposing a fast detection algorithm for urban road traffic congestion based on image processing technology. Firstly, to speed up the processing and to freely select the interesting area, the human-computer interaction vehicle area detection was put forward. Then, by using the difference of texture features between congestion image and unobstructed image, proposing vehicle density estimation based on texture analysis. Through image grayscale relegation, grey level co-occurrence matrix calculation and feature extraction, the energy and entropy features that could reflect vehicle density were obtained from vehicle area. After features training, the decision threshold could be obtained and traffic congestion was carried out.

Congestion Detection is used to detect a build-up of congestion in an area of interest (railway station platforms, public spaces, highway entry/exit slip roads, point-of-sale queues, etc.) This helps to initiate timely action and prevent an undesirable situation from worsening. It can also be used to provide statistics for staff planning and marketing purposes. For example, it can detect when a shopping mall is at its busiest, or when hypermarket queues start to build up.

#### 6.2.5.12 Video Management System (VMS)

S. No.	Minimum Requirement Description
VMS.FR.01	Video Management System (VMS) shall use the IP network as the platform for managing the entire surveillance system. End users shall have rapid access to relevant information for analysis.
VMS.FR.02	This shall allow operations managers and system integrator to build customized video surveillance networks that meet the city requirements. VMS shall be a scalable and flexible video management system that could be easily managed and monitored 10000 cameras in total.
VMS.FR.03	Scalable system shall permit retrieval of live or recorded video anywhere, anytime on a variety of clients via a web browser interface or media player. Video management server, on which the Video surveillance operation manager is hosted, shall manage the recording servers and IP cameras. Video management recording server shall record the feed of IP Camera installed at field locations. Video feed shall get recorded in video storage. Proposed storage box should be unified/NAS storage appliance with distributed architecture preferably. All the proposed IP Camera should provide with following functional specifications.
VMS.FR.04	Proposed intelligent video analytics software shall have the capability to provide various alarms & triggers and should notified if any incidence/violation happens. Various video analytics that shall be offered on identified cameras are: <ul style="list-style-type: none"> <li>• Person of Interest Origin Search</li> <li>• Unattended Object detection</li> </ul>

S. No.	Minimum Requirement Description
	<ul style="list-style-type: none"> <li>- Object tracking underneath the camera</li> <li>- Traffic Congestion Detection (by Avg Speed)</li> <li>- Wrong Direction Traffic Flow \ Congestion Detection</li> <li>- Wrong way driving</li> <li>- Indoor/Outdoor Trip Wire</li> </ul>
VMS.FR.05	The surveillance system shall provide a scalable and reliable platform to enable customized, network-based surveillance applications.
VMS.FR.06	The surveillance system shall be open standard supporting multiple vendor IP cameras and encoder manufacturers within the same system. The system shall support integration of ONVIF compliant cameras.
VMS.FR.07	The system shall support digital pan-tilt-zoom on live video. PTZ cameras should allow operators to use PTZ controls to zoom to a specific region in the viewing pane. Operators should select part of the full image and perform the PTZ controls within that region.
VMS.FR.08	The surveillance system viewing system should be in thick client for local viewing and thin client through http browser for remote viewing. Both thin and thick client shall provide the capability of viewing single or multiple live and archive cameras, control PTZ camera.
VMS.FR.09	VMS Review Player should support stand-alone Windows utility that plays video archive clips without a browser. The Review Player should also support MP4 files into a tamper-proof MPX (tamper proof MP4 file formats) formats .MPX file should include a password that is entered when the file is created. Application should ask the password to open and view the video file.
VMS.FR.10	VMS application should mobile application for Android & Apple devices such as the iPad and iPhone. App features should include recorded video playback, thumbnail video preview, and user profiles that allow multiple users to share a single device.
VMS.FR.11	The proposed surveillance system can be supported by the existing network infrastructure
VMS.FR.12	The System shall support the scalability of additional camera installation beyond the originally planned capacity. One single Video Management system shall be expandable to 10,000 cameras.
VMS.FR.13	The proposed video management system shall support deploying the software on Virtual servers, thus minimizing the hardware foot print for the project.
VMS.FR.14	The system shall have capability to stream video at remote sites by optimizing the bandwidth on WAN.
VMS.FR.15	The System should support automatic discovery and configuration, when any camera connect to network, the switch should recognizes the camera as a video endpoint, and then uses Smart Port macros to set the right network parameters for the video stream on the network.
VMS.FR.16	The system should allow users to access video streams from remote locations that have limited outbound bandwidth. The video should be delivered to multiple users without placing additional load on the remote locations.
VMS.FR.17	<p>The System should support Maps integration in future with below features;</p> <ul style="list-style-type: none"> <li>- Adding Image Layers to the location map.</li> </ul>

S. No.	Minimum Requirement Description
	<ul style="list-style-type: none"> <li>• Define the location map for each location.</li> <li>• Add cameras to the map images.</li> <li>• Add image layers to the map.</li> <li>• Add a Maps Server</li> </ul>
VMS.FR.18	System should support raster format images of jpeg/jpg and png file and Vector (shape files)
VMS.FR.19	Video Surveillance Storage System - The video surveillance storage system should support multiple options to store video. Servers, Direct Attached, shall augment server internal storage. The video surveillance storage system shall store video in loops, one-time archives, or event clips triggered by alarm systems. It shall support for RAID 6 storage.
VMS.FR.20	The system shall provide for integration with other software applications through an open and published Application Programming Interface (API). Such applications shall include, but not be limited to, access control, video analytics, and other alarm and sensor inputs.
VMS.FR.21	The system should ensure that once recorded, the video cannot be altered; ensuring the audit trail is intact for evidential purposes.
VMS.FR.22	All camera recordings shall have camera ID and location or area of recording and shall be programmable by the system administrator with user ID and password.
VMS.FR.23	System shall support camera template to define the resolution, frame rate, recording duration, and then apply to a group of cameras. The modification of the template will be reflected to all the cameras under the template.
VMS.FR.24	The system shall supports Bulk Action to allow to search and perform administration activities on multiple camera.
VMS.FR.25	The system shall support Bulk import of cameras from file such as excel/.csv, or other standard file format. The files shall include camera name, ip address, server, template, location, camera username and password
VMS.FR.26	The System should support LDAP (Lightweight Directory Access Protocol) server
VMS.FR.27	VMS System
VMS.FR.28	VMS System should have below application/ Console;
VMS.FR.29	<i>VMS Server Management Console</i>
VMS.FR.30	VMS Server Management Console should use by system administrators to perform infrequent administration tasks on a single physical or virtual machine. For example, use the Management Console to complete the initial server Setup Wizard, monitor system logs and resources, and troubleshoot hardware and system software issues, and gather information about the installed hardware and software components.
VMS.FR.31	The VMS Server Management Console user interface should available for each instance of system software installed on either a physical server or as a virtual machine.
VMS.FR.32	VMS Server Management systems should support network time protocol (NTP) on server, which automatically sets the server time and date.
VMS.FR.33	VMS Server Management Console should support configurable in a high availability (HA) arrangement that should allow a primary server to be paired with additional Failover, Redundant, or Long Term Storage Media

S. No.	Minimum Requirement Description
	Server. These HA servers should support the primary server with hot standby, redundant stream storage and playback, and long term recording storage to help ensure that functionality and recordings are not lost if the primary server goes offline.
VMS.FR.34	<i>VMS Operations Management Console</i>
VMS.FR.35	The VMS Operations Management Console should have browser-based configuration and administration tool used to manage the devices, video streams, archives, and policies for Video Management System deployment.
VMS.FR.36	The VMS Operations Management Console should have below features ;
VMS.FR.37	Manage physical devices - Add, configure and monitor the cameras, servers, and encoders that provide live and recorded video.
VMS.FR.38	Manage server services - Configure, enable or disable server services, such as the recording servers that manage video playback and recording.
VMS.FR.39	Monitor video - View live and recorded video, save video clips, search thumbnail summaries of recorded video, use the camera, Pan, Tilt and Zoom (PTZ) controls, or configure pre-defined video Views and Video Walls.
VMS.FR.40	Define recording and event policies - Create recording schedules, define event-triggered actions, configure motion detection, and other features.
VMS.FR.41	Monitor system and device health - View a summary of system health for all devices, or device status, alerts and events.
VMS.FR.42	The Health Dashboard has been enhanced to provide an overall snapshot of the recording servers, cameras and encoders in project deployment. System should provide view overall information, information about a specific device, or the estimated number of cameras that can be added to a recording Server, and other information.
VMS.FR.43	System should provide Storage for the total storage and used storage on the server, Existing Camera Count–The number of cameras currently added on the server.
VMS.FR.44	Backup and restore - Backup the system configuration, and optionally include historical data (such as alerts).
VMS.FR.45	The VMS Operations Management Console should support (if required) configurable as a redundant pair for high availability (HA) and system should ensure uninterrupted system access for users and administrators.
VMS.FR.46	<i>VMS Monitoring Console</i>
VMS.FR.47	VMS monitoring Console application should allow VMS System users to monitor live and recorded video.
VMS.FR.48	VMS monitoring Console should below viewing tool features;
VMS.FR.49	Operator can create video clips from multiple cameras using the Bulk Clipping feature. The clips can be automatically transferred to an FTP server, if necessary.
VMS.FR.50	Administrators should have hide live or recorded video from operator for specific cameras. System should allow to hide all live video streams, all recorded video, or recorded video for specific time spans.
VMS.FR.51	Operator should allow to pause live video streams by it should be enabled by default. Administrators should have option to disable this feature. Any user assigned to a user group with the Pause Live Video access permission can use the pause button when viewing live video streams.

S. No.	Minimum Requirement Description
VMS.FR.52	i. Desktop monitoring application
VMS.FR.53	Allows simultaneous viewing of up to 25 cameras per Workspace, and up to 48 cameras per workstation.
VMS.FR.54	Create Video Matrix windows for display in separate monitors.
VMS.FR.55	View Video Walls.
VMS.FR.56	Create unattended workstations.
VMS.FR.57	View and manage alerts.
VMS.FR.58	View cameras, video, and alerts based on a graphical map should support (if required)
VMS.FR.59	ii. Web-based configuration and monitoring tool
VMS.FR.60	Allows simultaneous viewing of multiple video panes:
VMS.FR.61	View up to 25 cameras with the 64-bit version of Internet Explorer.
VMS.FR.62	Add the users, Views and Video Walls available in the desktop application.
VMS.FR.63	Configure the camera, streams and recording schedules.
VMS.FR.64	iii. Desktop video clip player
VMS.FR.65	Simple player used to view video clip files.
VMS.FR.66	iv. Web-based server console
VMS.FR.67	Should provide basic viewing features for a single stream (Stream A) from a single camera.
VMS.FR.68	VMS monitoring Console should have below features;
VMS.FR.69	Client Application - A full-featured monitoring application should provide access to the cameras and video from a single screen should include the following workspaces and features: <ul style="list-style-type: none"><li>• Video workspace</li><li>• Wall workspace</li><li>• Alert workspace</li><li>• Maps workspace support (if required)</li><li>• Forensic Analysis Tools should support (if required)</li></ul>
VMS.FR.70	Video Player - monitoring application that includes the following monitoring workspaces: <ul style="list-style-type: none"><li>• Video workspace</li><li>• Wall workspace</li></ul>
VMS.FR.71	Video Wall Application – This should launches a monitoring application for unattended workstations. Unattended mode allows video monitoring windows to display Video Walls without access to the monitoring console configuration interface. The unattended screens should remain open even if the keyboard and mouse are disconnected, and can (optionally) re-appear when the workstation is rebooted.
VMS.FR.72	Forensic Analysis Tools - VMS monitoring Console should support below features
VMS.FR.73	Thumbnail Search–Use Thumbnail Search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search should display a range of video as thumbnail images, should allow to identify a portion of the recording to review.
VMS.FR.74	Clip Management–Use Clip Management to view, download and delete MP4 clips that are stored on the server.
VMS.FR.75	Motion Analysis–Use Motion Analysis to view a summary of motion events for recorded video.

### 6.3 Public Announcement (PA) System

S. No.	Minimum Requirement Specifications
PA-FR-01	The PAS can be used by ASCL, Police and other stake-holders of the project to disseminate information to road users/public.
PA-FR-02	The objective of the voice based sub-system is to disseminate the information to the citizens particularly during emergencies for the messages to reach quickly.
PA-FR-03	The system should have the capability of designing the messages based on the situation or context for broadcasting across PAS.
PA-FR-04	The software and solution of PAS shall comply with all functional and business requirement as specified in this RFP, elsewhere.
PA-FR-05	The PA system shall provide provision for emergency announcements to be made on per-location, selection of locations, or a system wide basis.
PA-FR-06	The PA system shall have provision for announcements to be made from two central locations.
PA-FR-07	The Integrated Traffic Management system shall provide for the ability to produce and play-out either pre-recorded messages or make live announcements through PA software.
PA-FR-08	The PA system shall be integrated with the Integrated Traffic Management & Emergency Response Management System for making automated, system generated, or manual announcements as per the SOPs.
PA-FR-09	The system should have ability to integrate with CCTV systems, other main/sub systems at COC for configuring and broadcasting the messages.
PA-FR-10	The system should have ability to configure the messages with the static or dynamic text from various applications/systems to form a complete message as and when required.
PA-FR-11	The system should recognize and broadcast messages based on some of the analytics such as sound alerts, system alerts, incident alerts and various other alerts.
PA-FR-12	The System should be able to integrate other networks PA system of third party application systems where the alerts are generated to broadcast messages.
PA-FR-13	There shall be an operator at central control room to operate the PAS application on PAS console.
PA-FR-14	The system should be able to generate various statistics, reports & MIS from time to time
PA-FR-15	The system shall be designed and installed so that it automatically minimizes community sound pollution
PA-FR-16	The requirements of local noise level standards & by-laws shall be respected by this system.

S. No.	Minimum Requirement Specifications
PA-FR-17	The system should have the ability to schedule category wise system messages or overall messages in advance for a period of time to selective or all PAS locations.
PA-FR-18	The PAS message quality shall be such that it is clearly audible from its location to a distance of more than 100m without any distortion and loss in quality of the sound during the prevailing situation in street.
PA-FR-19	Ability to integrate with CCTV systems, VMD and other main/sub systems at Command Centre for configuring and broadcasting the messages to the road users.
PA-FR-20	Ability to configure the messages with the static or dynamic text from various applications/systems to form a complete message as and when required.
PA-FR-21	Ability to categorize the messages as per the business need and able to configure as per category.
PA-FR-22	The PAS should provide the status indicators on the system and as well at various command centre
PA-FR-23	The PA system shall have an operations monitoring dashboard, located at the control centre
PA-FR-24	On this dashboard there shall be a schematic layout of the PA system showing all the connected nodes on the GUI.
PA-FR-25	The various nodes when connected & disconnected shall be represented in different colour schema on the GUI of the Control Centre operator.
PA-FR-26	If any particular node is disconnected from the control room, the same shall raise an alarm to the COC operator GUI & appropriate action shall be taken to rectify the same.
PA-FR-27	The monitoring dashboard shall allow the COC operator to click on any node & view the details of "Operator" logged in, time duration since logged in, summary of operations If COC operator or any other user from COC disable/enable/operate any active device remotely, the same shall be captured in COC activity report with all details including but not limited to date, time, device, action performed etc.
PA-FR-28	The monitoring dashboard shall show the status (connected/disconnected, faulty/working) of all logical devices (PA system) connected to a particular node when clicking on a node from the monitoring dashboard GUI.
PA-FR-29	In case of any fault in the devices connected to a node, or connectivity failure with a node, a pop-up message shall appear on the monitoring dashboard workstation. The operator has to acknowledge the pop-up message & report the type of fault to the maintenance team & shall record the details to the assigned team/individual into the system.
PA-FR-30	Fault assignment to the maintenance team shall be managed and controlled by the system software only. Once a fault is assigned by the COC 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

S. No.	Minimum Requirement Specifications
	maintenance team it shall be updated automatically (in case of active devices) or else updated manually in the software application/maintenance module.
PA-FR-31	The access to monitoring dashboard shall be specific to the privilege of the user which can be defined in the system & shall be specific to a group/part of node locations.

## 6.4 Emergency Call Box (ECB) System

- I. A high quality digital transceiver, to be placed at certain traffic junctions determined by the Police Department (mostly at junction boxes / camera poles to avoid any additional investments)
- II. Key is to make it easily accessible by public
- III. The unit shall preferably have a Double button which when pressed, shall connect to the Interim ICCC/ICCC/Police Command Centre/other locations over the existing network infrastructure setup for ITMS & Surveillance project
- IV. These are to be placed only at select locations such as Police/Traffic islands or pedestals or within the vicinity of constant Police supervision or IP camera field of view to avoid misuse and vandalism of the call box

## 6.5 Air Quality Monitoring System

### a. Air Quality Monitoring Stations

- I. Environmental sensor station shall monitor following additional parameters and include the following integrated sensors inside one station:
  - SO2
  - NO2
  - CO
  - CO2
  - O3
  - PM10
  - PM2.5
  - Noise pollution
  - Temperature
  - Humidity
- II. It shall be an integrated station which shall monitor overall ambient air, light and noise quality among other parameters as detailed in point above
- III. Air Quality monitoring station shall be ruggedized enough to be deployed in open air areas such as Industrial area, Markets, important bus stands and parks.
- IV. Air Quality Monitoring Systems shall be placed at approx. 6 locations in Amritsar as per [Annexure III](#).

### b. Central Environment System

- I. The Central Air Quality Monitoring software(AQMS) would be installed at the ICCC

- II. All Air Quality Monitoring stations shall be integrated with centralized monitoring software.
  - III. Software shall display real time and historical data in chart and table views for dashboard view of the Client
  - IV. Software shall display trends of environmental parameters based on user specific time periods
  - V. It shall be possible to configure and calibrate the sensors through the software from a remote location
  - VI. Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels
  - VII. Amritsar Smart City Limited should be able to configure or change the erroneous environmental parameters based on suggestion from stakeholders.
  - VIII. These Air Quality Monitoring stations shall sense the prevailing environment conditions and send the data to the AQMS, where real-time data shall be analysed, presented on dashboard with alerts.
  - IX. The AQMS shall also be integrated with the state and central pollution control board website and database via API integration to share data with them on regular intervals.
- c. Digital Display Unit
- I. The collated environmental information shall be relayed instantaneously to local Variable Messaging Sign Boards (VaMS) mounted on poles alongside the Air Quality Monitoring Stations which let citizens know the prevalent environmental conditions.
  - II. A Digital display software system shall be provided at the ICCC for message preparation, monitoring and control of the VaMS. The VaMS shall communicate with ICCC using an IP based network
  - III. The Digital display software application should accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client.
  - IV. Software should be GUI based, and capable to handle multiple VaMS. User should be able to select desired location on the Map and the live status of that specific Air Quality Monitoring Station and associated VaMS.

## 6.6 Water Quality Analyser

- I. Micro-Station for Quality Parameters Monitoring at ICCC
- II. The micro-station for waste water shall be supplied for online monitoring of water quality parameters in waste water. The required components: Spectro-probes and controller shall be the factory assembled with all required flow cells, mounting fittings and pipes on a compact panel
- III. The fully modular micro-station shall combine instruments to a compact and versatile system. It shall present a complete solution, as the user only has to connect water supply and -discharge ("plug & measure") in order to receive at no extra cost a previously unheard variety of immediately available information and

parameters. The micro station shall include terminals with monitoring tool software for data acquisition, data display and station control. The process connection shall be through PVC pipes with probes installed within flow cell. The micro station shall include compressor for pressurized automated cleaning

- IV. It shall provide the pressurized air for automatic cleaning of the probes. The device shall be designed for online monitoring of below mentioned quality parameters at Tung dhab and City Outfall drain
- V. The required components like the probes, controllers shall be factory assembled with all required flow cells, mounting fittings and pipes on a compact panel. Micro station data for quality parameters shall be integrated to IEG using Modbus RTU signal for local and remote monitoring
- VI. Following table describes the details of probe ranges, accuracy and the type of parameters to be measured at the Tung dhab and City Outfall drain.

**Waste Water Quality Parameters details with Probe ranges at the Tung dhab and City Outfall drain:**

S. No.	Parameters at Outlet	Unit	Treated Waste Water Limits at Outlet of STP	Probe Range	Accuracy	Treated Waste Water Limits
1.	Oil & Grease	mg/l	< 5	0 to 500	±2 %	< 5
2.	BOD (3 days 27 Degree C)	mg/l	< 20	0.01 - 20	±1 %	<10
3.	COD	mg/l	< 50	0 - 2000	± 2.5 %	< 50
4.	TSS	mg/l	< 50	0 - 1000	±2 %	< 10
5.	NH4-N	mg/l	< 5	0.05 - 20.0	±2 %	< 5
6.	pH	NA	6.5 to 9	2.0 - 12.0	±1 %	6.5 to 9
7.	DO	mg/l	> 2	0 - 50	±1 %	> 2
8.	Temperature	Deg C	Deg C	0-100	±1 %	< 5 Deg C Change

The major prerequisites of efficient online analysers are as follows:

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

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

This spectrophotometer records light attenuation in the wavelength region between 200 and 750 nm. The measurement is performed in-situ, without sampling or sample pre-treatment, thus preventing errors due to sampling, sample transport and storage etc. A measurement cycle takes between 20 and 60 seconds, making possible a high measuring frequency and detection of rapid changes

## 6.7 Integrated Command Control Centre

### 1.1.1 ICCC Platform Overview

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

Command and Control Centre with robust IoT Platform involves leveraging on the information provided by different devices/ platforms & various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city.

Under the Amritsar smart City Initiative it is intended to cover and integrate various disparate systems including:

- I. City Surveillance
- II. PA system
- III. Emergency Call Box
- IV. Fleet Management
- V. Water Sensor analysers
- VI. Air Quality Monitoring Stations
- VII. Integrated Dashboard for City Officials
- VIII. Variable Message Displays (Future Phase)
- IX. E-governance Applications (Future Phase)
- X. Intelligent Traffic Management System (Future Phase)
- XI. Smart Parking (Future)
- XII. Smart Lighting (Future Phase)
- XIII. Environmental Sensor ((Future Phase)
- XIV. Solid Waste Management system (Future Phase)
- XV. Citizen Mobile App (Future Phase)
- XVI. Integrated Utilities Management (Energy , Water and Gas) (Future Phase)

#### 6.7.1 ICCC Platform Functional Requirements

- I. The Platform shall be a fully integrated portal-based solution that provides seamless incident-response management, collaboration and geo-spatial display.
- II. The Platform shall provide real-time communication, collaboration and constructive decision making amongst different agencies by envisaging potential threats, challenges and facilitating effective response mechanisms. Thus, the platform shall provide a Common Operating Picture (COP) of various events in real-time on a unified platform with the means to make collaborative and consultative decisions, anticipate problems to resolve them proactively, and coordinate resources to operate effectively.
- III. The platform should have high processing power and adequate data storage with a high performance information highway to provide process information in real time and serving decision support system. The platform should also provide portability to meet changing city scenario. The MSI is required to provision data storage and processing power of the platform adequately to meet the system design and functionality to be achieved.
- IV. The solution should be capable of seamless integration to various government and emergency services such as law enforcement, disaster and emergency services, utility services etc.
- V. The platform shall support adding more layers of solutions seamlessly with minimal effort which the municipality/development authority intends to develop in time to come (But not limited to mentioned solution only).
- VI. On the ICCC platform, the system shall provide Standard Operating Procedures (SOPs), step-by-step instructions based on the Authorities policies and tools to resolve the situation and presents the relevant situation information in a quick and

- easily digestible format for an operator to verify the situation. The system shall provide reporting & audit trail functionalities to track all the information and monitor operator interactions with the system and to impart necessary training to the users.
- VII. The inputs/feeds from the different components of Smart City Solutions shall be received at Integrated Command and Control centre video wall for monitoring, tracking and decision support purpose on real time basis supported with GIS technology. Further, operators shall be working on their respective monitors for assessing the inputs and triggering actions at ground level.
  - VIII. MSI needs to conduct a detailed assessment, design a comprehensive technical architecture, implement and operate the common Integrated Command & Control Centre Platform.
  - IX. The proposed Integrated Command & Control Centre Platform shall be hosted at data centre and all field level smart cities use cases needs to be integrated with this platform. City level applications like ERP, E-governance, taxes and all other business application shall also be integrated with ICCC platform to read & analyse data from those application to visualize on ICCC dashboard.
  - X. Proposed ICCC architecture should be combination key functionalities like Data Normalization, IoT Platform, API Manager/Gateway, Database and City operation centre software.
  - XI. Data Aggregation & Normalization Layer must integrate City urban services as per current & future need of city and must deliver an architecture which shall be future scalable to accommodate more urban services & Applications.
  - XII. Data from this aggregation & normalization layer shall be used for urban services/applications management & Control & customized Reporting's. Also, this layer should provide the data to various cities partners/application developer's via API to develop citizen centric applications, portal and mobile applications etc.
  - XIII. MSI needs to conduct a detailed assessment, design a comprehensive technical architecture, implement and operate the common Integrated Common Command & Control platform.
  - XIV. All field level smart cities use cases needs to be integrated with this platform. City level applications like ERP, E-governance, taxes and all other business application (In future) shall also be integrated with platform to read & analyse data from those application to visualize on City level CCC (Command & control Centre) dashboard
  - XV. Proposed Solution architecture should have combination of data normalization (IoT Platform) and City operation centre software functionalities covering Complex Event Processing, Rules Engine, Map and Video Based Visualization.
  - XVI. Data Aggregation & Normalization Layer must integrate City urban services as per current need of city and must deliver an architecture which shall be future scalable to accommodate more urban services & Applications.
  - XVII. Data from this aggregation & normalization layer shall be used for urban services/applications management & Control and customized reporting's.

### 6.7.2 Network Operation Centre (NOC) Function Requirement

- I. NOC shall monitor all the infrastructure devices (Router, switches, firewall, advance security component, bandwidth, Application performance etc.) that are kept in core locations, aggregation layer along with key services that shall be provisioned in due course.
- II. NOC Shall help in monitoring the issues related to fiber, network, and infrastructure implemented, Applications and Platforms and provide help desk system for the same.
- III. Configurations and Change Management: Configuration shall be managed from core locations for all the devices/sensors on the network. For any change applicable, based on the type/severity/complexity of change, the change should be proposed with due justification and to be implemented upon approval from ASCL.
- IV. The proposed solution shall be scalable in nature to host all key services under smart city.
- V. The proposed solution shall have redundancy built at each layer.
- VI. The proposed solution shall be ready to scale up both horizontally and vertically.
- VII. The proposed solution shall be ready in all respect where it is envisaged by ASCL to make use of this infrastructure under different revenue models under its long-term vision.
- VIII. The solution shall meet demands of bandwidth needs for all the procured and planned smart city solutions in near future (Applicable for Core component in Data center)
- IX. The key functionalities of the NOC shall include
  - Incident Management based on resource workload, incident Category etc.
  - Tracking and reporting of all contractual SLAs in an automated way.
  - Updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
  - The NOC shall escalate issues in a hierarchical manner, so if an issue is not resolved in a specific time frame, the next level is informed to speed up problem remediation.
- X. Primary responsibilities of NOC personnel shall include but not limited to:
  - Network Supervision and Monitoring: Monitor the complete network 24/7, to keep network and systems functioning in a stable operation mode
  - Configuration Management: Ensure the proper configuration of network, systems and applications or the provision of reliable and high quality end-user services
  - Change Management, Network Extension: Ensure efficient day-to-day management of short-term network changes and optimization, including their implementation. This activity shall be synchronized with the maintenance scheduled activities
  - Performance Management: Provide efficient performance management procedures ensuring a reliable, high-quality network performance and service
  - Service and Network Provisioning: Define all necessary actions to be performed when a request for a new service is issued, and control the actions performed at NOC level or field level until completion

- Scheduled Activities Planning: Provide regular plans for all scheduled activities, including preventive maintenance. Respect a schedule, and achievement of the plan. This is linked to the change management function which ensures overall synchronization of all network activities
- IT and DB Management: Day-to-day management of all OSS systems, IT systems and databases (administration, backups)
- Security Management: Define and implement security policies, guidelines, and best practices, and check for compliance with security regulations
- Quality Management: Define quality management policies, and ensure implementation and usage for competitive quality of service
- Workforce Management : Manage field personnel to ensure timely interventions and respect of the preventive maintenance plan
- Inventory Management : Ensure consistent management of network equipment, and accurate, up-to-date documentation of it
- Spare Parts Management : Manage spare part handling and logistics to minimize repair/swap turn-around times for defective items, & keep low CAPEX for spare parts and consumables
- Asset Inventory Management : Ensure consistent inventory management for all assets including infrastructure, buildings, tools, spares, and equipment
- Repair and Return: Receive and repair defective boards, return repaired or replacement boards.

XI. The MSI shall ensure adherence to the following prerequisites:

- All the IT devices that are installed by the MSI shall be Simple Network Management Protocol ('SNMP') enabled and the MSI shall centrally and remotely monitor and manage the devices on a 24x7x365 basis. It should also be provisioned to bring Non-IT components on the common monitoring
- MSI shall provide on-site comprehensive maintenance of the entire IT / Non-IT Infrastructure and their components supplied with a provision of onsite spares on 24x7x365 basis after successful execution and acceptance of respective project phase. The individual project phases will run independently.
- MSI shall operate and maintain the Network infrastructure (Active / Passive / Physical) as per well-defined Standard Operating Procedures.
- MSI to establish and implement leading practices of IT service Management like Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO)/IEC 20000 standard that shall promote the adoption of an integrated approach to effectively deliver managed services to meet the requirements.
- MSI shall identify all assets and document the importance of these assets. The asset inventory shall include all the information necessary in order to recover from a disaster, including type of assets, format, location, backup information, license information etc.
- MSI shall undertake scheduled and ad hoc maintenance (on need basis) and operations like configuration backup, patch management and upgrades
- MSI shall establish basic tools for IT and Non-IT management to undertake health check monitoring, troubleshooting etc. for all Network operations
- MSI shall establish access control mechanism and shift wise attendance management system

- The MSI shall ensure that all resident engineers in the NOC are certified (of the OEMs of the network components) and are provided at Command and Control Center for 24/7 operations.

XII. Typical Network Infrastructure Management Services shall include

- MSI shall ensure that the network is available 24x7x365 as per the prescribed SLAs
- MSI shall provide services for management of network environment to maintain performance at optimum levels.
- MSI shall be responsible for attending to and resolving network failures and snags
- MSI shall support and maintain overall network infrastructure including but not limited to WAN/LAN passive components, routers, switches, Firewalls', IPS/IDS, Load Balancers etc.
- MSI shall Configure and backup network devices including documentation of all configurations
- MSI shall provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers
- MSI shall create required facilities for providing network administration services including administrative support for user registration, creating and maintaining user profiles, granting user access and authorization, providing ongoing user password support, announcing and providing networking services for users.
- MSI shall provide a single-point-of-contact for requesting any service. The Network Administrator shall respond to the initial request from the user groups within the agreed service levels and service coverage hours.
- MSI shall provide support as required to assist in hardware and software problem isolation and resolution in the LAN/WAN environment.
- MSI shall perform LAN/WAN problem determination.
- MSI shall communicate changes affecting the LAN/WAN environment.
- MSI shall maintain LAN/WAN configuration data.
- MSI shall be responsible for polling / collecting of network devices security logs from all the systems. All these logs shall be made available to the Enterprise Management System (EMS) solution

XIII. Security Administration and Management Services:

- Management of security environment of the entire network infrastructure to maintain performance at optimum levels.

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

#### XIV. Physical & Environmental Security at locations

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

#### 6.7.3 Data Centre Functional Requirements

- I. Amritsar Smart City Data centre architecture shall categorized in three zones with the help of Spine and leaf architecture as per below mentioned.
  - External zone shall consist of termination points for Internet & City WAN Network ISP links and a DMZ zone that shall be create for accessing the public servers from internet.
  - Internal zone shall consist of a MZ & DMZ zone where all Security, Collaboration, Monitoring, Application performance and management devices shall be placed

- Compute & Storage Network where all Compute hardware & Smart city application software, Surveillance & unified storage and Backup appliance shall be placed
- II. Proposed solution shall meet the minimum following
- Internet Links shall be terminated at internet routers in high-availability mode
  - City WAN network shall be aggregated into ISP links that shall be connected at Core router in high-availability mode and MSI should include required number & type of Ports in the core router to terminate the WAN ISP links with some spare ports for future use.
  - Internet firewall shall be proposed with Next Generation Firewall including IPS & Anti-APT functionality to protect the data centre network from internet born threats and shall be placed at perimeter level.
  - Core firewall shall be placed at between core network components and internal data centre as a 2nd layer of defence of the data centre network
  - Network Behaviour Analysis flow collector & sensors shall be placed at perimeter level for continuous real-time monitoring & pervasive view of all network traffic.
  - Data centre switching architecture shall be based on spine-leaf architecture wherein all the devices should connect to leaf switches and Spine switch should connect to leaf switches over high speed connectivity
  - All the L4-L7 devices (Anti-APT, Server Load Balancer, WAF, Policy Server, NBA, EMS etc.) shall connect to Leaf switches over multiple 1/10G Ethernet links.
  - The compute infrastructure shall also connect to leaf switches over multiple of 10G connectivity's
  - Surveillance and Unified Storage shall connect to leaf switches or compute infra through SAN switch as per solution

#### 6.7.4 Cyber Security Framework

A smart city is an intelligent interconnection of people, processes, data and things. A smart city uses digital technologies or information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens.

Smart cities use a variety of sensors to digitize various forms of information, and carry the digital data over a transport network to a data centre, where the data is processed and analysed using different tools, and viewed by operators in the central command and control centre.

Integrated Command & Control centre personnel also use the standard IT infrastructure for a variety of services like Internet access and email services. The Internet access is also provided into the data centre of the smart city for access to specific applications for disseminating information, or carrying out digital transactions.

ICCC is the place where all of the applications would reside and process the data generated by the millions of sensors across the city. Any security breach into the ICCC would lead to

loss of data or data being manipulated. This needs to be prevented by having a proper security architecture in place for the ICCC.

Segmenting ICCC into multiple zones with each zone having a dedicated functionality e.g. all sensors for one Operational domain can connect to the ICCC in one zone, and the Internet facing side of the ICCC shall be in another zone. This would ensure that any disturbance/breach in one functional domain does not impact the other domains. All communications between these zones has to be controlled through dedicated firewalls.

Internet facing part of the ICCC shall have a Demilitarized zone where all the customer application servers would be located that are customer facing. Only these servers can access the data from the actual utility application servers on predefined ports. Further, the customer application servers would be accessed only by the web server that is hosted in a different zone of the ICCC.

In addition to the firewalls, and Intrusion detection & Intrusion prevention systems that are being used in the ICCC, Behavioural analysis device shall be deployed in the ICCC to look out for any abnormal behaviour as defined by the administrator or a behaviour that is different from normal network baselines.

Security devices deployed in the ICCC shall be able to use global threat intelligence and be able to use that knowledge in detecting any attacks on the ICCC infrastructure. The system shall also be able to correlate this threat intelligence with advanced threat analytics and provide intelligent actionable information.

Next, a Denial of Service prevention device shall be used within the ICCC to ensure that the user services are not disrupted by overwhelming the devices in the ICCC by sending malicious traffic.

Finally, a strong security team needs to be built that can take the alerts from the different security elements, to provide a cohesive view of the overall security posture of the Smart city infrastructure and to detect any threats based on global threat intelligence from threat intelligence sources, to be able to take proactive action to prevent any data/ service loss.

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

Area of focus	Description	Devices/ Technologies
Access Security	Protecting against unauthenticated devices from sending information to the Integrated Command & Control Centre (ICCC).	Authentication, Authorization and Accounting (AAA)
Transport Security	Prevent any eavesdropping on the network by sniffing data on the network.	Access control and secure encrypted transport over network like Leased line/ SDWAN/MPLS networks

Area of focus	Description	Devices/ Technologies
ICCC Security	<p>Preventing any illegitimate traffic from entering the ICCC from the access network.</p> <p>Preventing attacks on one component of the ICCC solution from impacting other solutions/ components.</p> <p>Preventing any unauthorized access into the ICCC from the Internet through emails, or web browsing.</p> <p>Base lining the normal traffic patterns in the smart city network infrastructure and detecting for any deviations from the baseline.</p> <p>Preventing against any malicious files that can transform after coming into the network (Advanced Persistent Threats).</p> <p>Preventing users and systems from within the ICCC to access any malicious sites even before they initiate the request.</p>	Internet & Internal Firewall. Network Behavioural Analysis and Detection. Web security devices. Anti-APT solutions on network perimeter like email and web gateways.
Services Security	<p>Ensuring that the smart city services are always available to the users/ citizens, and are not impacted by any DDoS attacks.</p>	Application DDoS protection systems.
Security Operations	<p>Ensuring that the security logs are analysed proactively, and the traffic and data patterns analysed for proactive threat hunting.</p> <p>Ensure that if a security incident occurs, it is detected, contained and mitigated in a fast and effective manner so as to prevent the spread of the infection.</p>	Managed Detection and Response Services coupled with threat intelligence services by MSI.

As per the minimum-security requirements below are the devices which will be required as minimum

#### 6.7.4.1 Network Behaviour Analysis & Detection

MSI shall propose required solution for automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts. Also shall capture signature / heuristics based alerts and block the same.

Network Behaviour analysis is an Integral part of today's cyber security solution as it provides entire visibility of network like who is doing what etc. Some of the Functional Features that shall provide visibility into network and detect threats proactively are as below:

- I. Visibility & Identity Awareness
  - a. NBA Solution shall provide the internal network visibility and actionable insight required to quickly identify and troubleshoot a wide variety of network issues. Additionally, NBA integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.
  - b. NBA Solution shall also collect and analyse device through integration with the AAA devices.
- II. Troubleshooting
  - a. NBA Solution shall also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution.
  - b. BYOD & Mobile Devices
  - c. NBA Solution shall monitor users and mobile devices on the network, including personal smartphones, tablets and laptops. Mobile awareness helps pinpoint the exact source – even USB drives – of issues such as zero-day attacks, insider threats, policy violations and data leakage.
- III. Forensics and Incident Response
  - a. By collecting, analysing and storing large amounts of flow data, NBA System provides a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.

#### 6.7.4.2 Authentication, Authorization and Accounting (AAA)

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

#### 6.7.4.3 Internal and Internet Firewalls

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

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

#### 6.7.4.4 Intrusion Prevention system

- I. The IPS shall accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, Do's, DDoS, vulnerability exploitation, hybrids, and zero-day attacks, Worm, Phishing, Spyware, Virus, Trojan, P2P, VoIP, Backdoor, Reconnaissance, Bandwidth Hijacking, Cross-site scripting, SQL Injection, malformed traffic etc.
- II. Shall detect and block all known, high risk exploits along with their underlying vulnerability and not just one exploit of that vulnerability.
- III. Shall support traffic inspection for IPv6, IPv4, and Tunnelled: 4in6, 6in4, 6to4 traffic.
- IV. Support for ingestion of threat intelligence feeds like IP reputation intelligence feeds, URL & DNS threat intelligence feeds and SNORT signatures.
- V. Shall have an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

#### 6.7.4.5 Web Security Solution

With the emergence of Web 2.0 and social media, web has become very important threat vector for cyber criminals. We have envisaged that web security shall be important aspect of our cyber security solution and shall have following critical features:

- VI. Appliance Requirement and Functionality: Shall be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities shall be in a single appliance only. Option to run Advance Malware Protection engine utilizing sand boxing technology for file and file reputation analysis.

- VII. Secure Remote Access: Critical feature of the solution as web security shall be deployed across an organization. Support Team shall be able to login to appliance using secure tunnelling methods such as SSH for troubleshooting purposes.
- VIII. Forward proxy mode - Single and Dual IP configuration: Forward proxy mode deployment solution to support single / Dual IP proxy configuration where one IP will be of local LAN and another IP will be of DMZ.
- IX. Support multiple deployment options: The solution shall allow to deploy the appliance in explicit proxy as well as transparent mode together.

#### 6.7.4.6 Anti-APT

Advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization. Bidder shall provide solution which is capable of working in Inline Blocking mode without depending on other network components like a separate FW, IPS or Web Security Appliance.

#### 6.7.4.7 Web Application Firewall

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

#### 6.7.5 Seating Capacity and IT/Non IT Equipment

S. No.	Room Description	Expected Seating capacity	Mandatory or optional	Tentative Computer Equipment
1.	Reception	1 Person	Mandatory	Personnel Computer with Visitor Management Logging- 1 No. with a Monitor
2.	Police Function Control Room with Gallery option	12 People - 10 Operator and 2 Supervisors	Mandatory	Personnel Computer with work stations - 10 Nos with 3 Monitor for each PC. Heavy Duty All in one Printer - 1 No. Video Wall 4X3 50"Cube - 1 No. / IP Phones - 12 No.
3.	Municipal Functions control Room with Gallery Option	12 People - 10 operator and 2 Supervisors	Mandatory	Personnel Computer with work stations - 12 Nos. with 3 Monitor for each PC. Video Wall 4X2 50"Cube - 1nos / IP Phones - 12 No.
4.	Data staff centre - PM, Server, N/w,	16 People	Mandatory	Work Stations or Laptop for 16 People as per requirement

S. No.	Room Description	Expected Seating capacity	Mandatory or optional	Tentative Computer Equipment
	Security, Help desk, Application Development/s upport staff & ICCC Staff etc.			
5.	Data centre - Farm Area (4 Racks)	4 Racks with space for expansion to 10 racks	Mandatory	Including server and network racks
6.	Telecommunications Room	1 telecom racks with space for expansion to 4 racks	Mandatory	Including server and network racks
7.	Conference Room/War Room	20 People with LAN connectivity	Mandatory	Video Conference Equipment, 20 People Seating capacity with furniture. Size may be reduced if required in final design.
8.	Staging room	1 Rack and 1 Personnel computer	Mandatory	Rack -1 and PC -1
9.	Power Distribution Panel Room & Battery Room	Switching panels and electrical devices	Mandatory	-
10.	Building Management System Room with staff	5 People including supervisor.	Mandatory	Personnel Computer - 5 Nos. with BMS Systems
11.	PAC in the farm area	3 nos. or as per requirements	Mandatory	-
12.	DG with Fuel Tank	1 nos. or as per requirement	Optional	-
13.	Sub Station / Transformer	2 nos. or as per requirement	Optional	-
14.	Earth Pits	As per requirement	Mandatory	-

#### 6.7.6 Non IT - Civil Infrastructure: Guidelines and Specifications

S. No.	Nature of Requirement	Guidelines / Specifications
1.	Site Survey	i. The MSI shall perform detailed site assessment and survey to design, implement, operate and maintain the ICCC and DC.

S. No.	Nature of Requirement	Guidelines / Specifications
2.	Demolishing & Dismantling Works	<p>i. Removing and Dismantling of existing walls, false ceiling, existing Aluminium windows &amp; ventilators with glass on, Brick walls, Doors, partitions, including, associated wiring, etc. in order to suit the Proposed Layout and carting away the debris from the site. Necessary care shall be taken to ensure minimum damage to the existing materials. All dismantled salvageable items shall be neatly stacked in a designated area within the compound as directed by the Client.</p>
3.	Site Preparation	<p>i. Providing and construction of Brick wall - 230 mm thick using best quality bricks in cement mortar 1:4. The rate shall be inclusive of all material, labour necessary scaffolding and Pointing, lifting, curing and other charges if any etc. all complete</p> <p>ii. Providing and construction of Brick wall - 115 mm thick using best quality bricks in cement mortar 1:4 with proper reinforcement bands at every 1m height intervals, and also match with existing wall surface both inside and outside. The rate shall be inclusive of all material, RC lintels at required levels for full-height construction, labour, necessary scaffolding and Pointing, lifting ,curing and other charges if any etc. all complete</p> <p>iii. Closing of existing windows along the ICCC and Data centre periphery with Brick work - 230 mm thick using best quality bricks in cement mortar 1:4. Brick work in window / Ventilator area should be constructed with water tight and also match with existing wall surface both inside and outside. The rate shall be inclusive of all material, labour necessary scaffolding and Pointing, lifting, curing and other charges if any etc. all complete</p> <p>iv. Providing Anti termite treatment before starting brick work area with ISO brand chemical approved by ASCL or Consultant. The rate inclusive of labour &amp; material all complete</p> <p>v. Providing and laying 12mm thick internal plaster on brick walls in cm ratio of 1:4. Rate shall be inclusive of providing and fixing scaffolding to the necessary level with necessary safety arrangements</p> <p>vi. Providing and laying external plaster on brick walls in 2 layers. First layer shall be 12mm thick in 1:4 ratio cm mixed with waterproofing compound and second layer of 8mm thick in 1:3 ratio cm mixed with waterproofing compound. Rate shall be inclusive of finishing the</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>exterior surface with matching exterior weatherproof paint of existing type and shade. Rate shall be inclusive of providing and fixing scaffolding to the necessary level with necessary safety arrangements</p> <p>vii. Providing &amp; laying cast-in-situ controlled reinforced cement concrete of the designed grades using 20 mm and down size coarse graded machine crushed hard stone aggregate including designing the mix, weigh batching, mechanical mixing, transporting and placing at all lifts, vibrating, consolidating, curing and finishing smooth as required all exposed faces, complete for the following RC structural and other elements including centring, shuttering, form work either straight, curved, plain, tapered or sloped, supplying and mixing admixtures, dewatering wherever necessary, the cost of all complete materials, labour, all leads and lifts, tools, plant and machineries, hire and fuel charges and all other incidental charges etc., complete. The designing of concrete mix for different grades of controlled concrete should be done in accordance with latest IS - SP 23. (Hand book on concrete mix design) in the field laboratory and the same should be got approved by the Engineer. Rate shall include providing and fixing reinforcement for the following RCC work with Thermo mechanically treated (TMT) bar of various diameters and grade of steel as designed for the imposed loads conforming to IS or equivalent BS specification including cutting and waste, bending, hoisting, fabricating and placing in position and binding the reinforcement with galvanized annealed binding wire of double fold of 18 gauge and providing PVC cover blocks for placing the reinforcements in position and for maintaining the cover specified and/or according to relevant IS or equivalent BS code</p> <p>viii. Construction of structurally designed RCC Civil foundation platform, each of approximate size of 8.2 meters by 3meters &amp; 1.2 meters depth for housing the proposed DG (2 x 630 KVA) with a static load 10 tons &amp; dynamic load of 18 tones. Rate shall include supply and fixing of required base plates, etc. for supporting the DG at required locations, complete in all respects</p>
4.	Carpentry/Furniture - Cabinets/Storage	<p>i. Providing and fixing Filing storage unit of 900 (W) x 450 (D) x 2100 mm (H) in the BMS room but in general, it shall be made out of 19 mm thick commercial plywood on all sides. The storage unit shall include adjustable intermediate shelves made of 19mm comm. Plywood</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		placed on necessary S.S stud supports. The openable shutter shall be made out of 19mm thick comm. plywood with necessary teakwood supports etc. complete. Rate shall include for providing teak wood moulding of size 40 x 15mm at top level etc. complete. All exposed surfaces shall be finished with 1mm thick laminate of approved shade and all inner / recessed surfaces shall be painted with sealer finish. Rate to include all hardware, tower bolt, magnetic catch, heavy duty hinges, S.S handles - of approved make, including locking arrangements with master key of approved make etc. complete
5.	Modular Furniture for DC staff & ICCC staff	<p>Single-sided W/s row - size 1200 x 600mm, 60mm thick partition of height 1200mm; Data raceway at skirting level; Power raceway at below table-top level; 25mm thick laminate table-top with post-formed edges; individual 3-drawer mobile pedestal storage unit; Pin-up soft boards with approved colour felt cloth; Keyboard tray; CPU trolley; Gable end support;</p> <p>Double-sided W/s row - size 1200 x 600mm, 60mm thick partition of height 1200mm; Data raceway at skirting level; Power raceway at below table-top level; 25mm thick laminate table-top with post-formed edges; individual 3-drawer mobile pedestal storage unit; Pin-up soft boards with approved colour felt cloth; Keyboard tray; CPU trolley; Gable end support;</p> <p>Running Table-top counter in Staging area - 25mm thick countertop with Laminate finish and Post formed edges with required intermediate Gable ends; 2 nos. of mobile 3-drawer pedestal storage unit</p> <p>Running Table-top counter in Help Desk room - 25mm thick countertop with Laminate finish and Post formed edges with required intermediate Gable ends; 3 nos. of mobile 3-drawer pedestal storage unit</p> <p>Running Table-top counter in BMS room - 25mm thick countertop with Laminate finish and Post formed edges with required intermediate Gable ends; 1 no. of mobile 3-drawer pedestal storage unit</p> <p>Meeting Table - 10-seater; Size 3000 mm x 1500 mm; 25mm thick countertop with Laminate finish and Post formed edges; and 2 sets of required concealed Flip-top boxes for Electrical and Data outlets.</p>
6.	Partition Type 1	i. Providing and fixing in position of 75 mm thick Gypsum board partition using 12.5 mm thick gyp-

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>board single skin on both sides with G.I steel metal stud frame of size 48 mm thick using floor and ceiling channels of 50 mm thick i.e. 0.55 mm thick and having equal flanges of 36 mm with GI stud 48 mm width i.e. 0.55 mm thick and having one flange of 36 mm placed @ every 600 mm c/c in vertical direction upto ceiling and the ends should be crimped / screwed rigidly at top and bottom etc. complete. Rate shall include to stiffen the partition horizontally with GI fixing channel of 0.99 mm thick, 99 x 2440 mm long size and screw it on either side of the G.I frame etc. and also ensure that the stud frame at the top level of the joinery opening with joints staggered to avoid continuous joints etc.</p> <p>ii. Fixing of channels shall also provide for suitable attachment of fixtures to the partitions and the perimeter opening should be trimmed with G.I metal studs packed with best quality treated Malaysian Sal wood to required size and shape with 2 coats of fire proof paint over a coat of anti-termite treatment / anti-corrosive primer to receive screws / anchor fasteners to fix Joinery frame in position etc. complete. Rate shall include Gypsum board on both sides of the frame work vertically spanning from floor to ceiling fixed with drywall screws to a suitable diameter and length at every 300 mm c/c. The screws should be of zinc chromium plated, self-drilling etc. The joints between the gyp-boards shall be finished flush and even with jointing compound and paper tape and the surface shall be painted with 2 coats of plastic emulsion paint of approved make and shade over a coat of primer suitable for gyp-board after E-Mix / P.O.P / Gypsum putty and all as per manufacturer's specification etc. complete and all as directed. Rate shall include necessary arrangement to ensure proper anchorage / fixing from the ceiling to get sufficient rigidity (to the required level)</p> <p>iii. Rate shall include fixing of 100 mm high recessed skirting made out of 12mm tk. Comm. Ply and finished with 1 mm laminate of approved shade</p>
7.	Type 2 Partition	<p>i. Providing and fixing glazed partitions of 10 mm thick toughened glass as per basic First floor layout drawing using S.S Patch fittings. Rate shall include for transport charges, handling, loading and</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		unloading, installation of glass and clear sealant between butt joints and perimeter on all sides
8.	Type 3 Partition	<p>i. Providing and fixing running glazing for Vision panel within the partitions along the Tech Support room of 10 mm thick clear glass as per basic first floor Layout drawing. 12 mm thick MDF beading finished with paint of approved shade shall be used to fix the glass. Care shall be taken to paint the inner faces of the MDF beading before fixing the glass. Rate shall include for transport charges, handling, loading and unloading, installation of glass and clear sealant between butt joints and perimeter on all sides.</p> <p>ii. Providing and fixing vertical blinds with 89 mm wide imported superior polyester base fabric vanes with Scotch guard application as per approved sample and the ranges of louver shall be in 'Select and Classic'. The vertical blinds shall have a head rail of extruded anodized high strength aluminium alloy, shall be 25 mm x 50 mm high or equivalent with gauge thickness of 1.2 mm or equivalent. End control units consist of reduction gearbox having the reduction ratio of 3.5:1 for a very smooth operation of the blind. This unit shall consist of planetary gear in the outer housing, four small transmission gears fitted in the middle assembly and an end receiving gear attached to central sprocket unit. Tilter chain is made of 4.5mm plastic beads moulded on 2.2mm thick polyester card</p> <p>iii. The pitch of the beads shall be 6mm. The end control unit shall have the facility to rotate the louver by 180 degrees. Tilt rod shall be made of extruded aluminium having 3 keyways and the average dia shall be 5.8 mm. Carrier (Runner) shall be made of moulded plastic having anti-friction additive. It shall consist of polymer housing with wheels mounted on sides &amp; shall have a gear and worm mechanism with vertical worm fixed with a tongued poly-carbonate stem to hold the louvers.</p> <p>iv. The vanes shall be capable of 180 deg. rotation in position and shall be of polyester / viscose yarn dyed in fast colours a strain resistant chemicals treatment or equivalent protective coating shall be applied on vanes. The installation shall be complete in all respects</p> <p>v. Providing and fixing soft board panel of specified sizes having 12 mm thick soft board covered with felt fabric of approved make and shade of premium quality .The board shall have teakwood/cedar/beech/matching wooden beading, lipping around. The board shall be fixed on prepared</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>surface with necessary hardware fittings etc. complete. All concealed wood works shall have sealer polish as directed. Rate quoted shall be for the complete finished work including all the materials and labour mentioned above</p> <p>vi. Providing and fixing Glass Writing Board with S.S studs inclusive of all taxes, surcharge, duties, etc. Rate shall be inclusive of delivery and installation, and all material and labour. a) Size of 6'0" x 4'0" (NOC Room)</p>
9.	Glass Etching	<p>i. Providing frosted etching to glass panels using 3M stickers of "sparkle" type as per approved design and as directed</p>
10.	False Ceiling	<p>i. Providing and fixing seamless ceiling with Gypboard of 12.5 mm thick, fixed to the underside of the suspended grid formed of GI perimeter channel of size 20 x 27 x 30 mm (MF 6A) fixed along the wall by using wood screws and metal expansion rawl plugs. The GI intermediate channel of size 45 x 15 x 0.90 mm (MF7) shall be fixed to the suspended strap hanger / GI ceiling angle at intervals not more than 1220 mm. The suspended GI ceiling angle / Strap hanger is to be connected with GI soffit cleat of size 37 x 27 x 25 x 1.6 mm and it should be fixed on the roof slab / beam, by using metal expansion fasteners of 12.5 mm dia. to a length of 35 mm with 6 mm dia. bolt / screw at top ends</p> <p>ii. The GI ceiling section of size 80 x 26 x 0.5 mm (MF 5) is to be provided across the intermediate channel at intervals not more than 457 mm centers at bottom and the same shall be fixed by GI connection clips 2.64 mm dia. at the intersection points. The ends of ceiling section (MF 5) channel by adopting an overlap length of minimum 150 mm, connected with intermediate channel shall be fixed to perimeter channel in insertion. The Gypboard shall be fixed to the underside of the suspended grid by using 25 mm long drywall screws. The joints shall be finished with joint paper tape by using jointing compound and applying over it 3 layers of the filler compound to provide a smooth surface. The ceiling surface shall be painted with two coats of approved first quality plastic emulsion paint, after applying a coat of primer etc. complete. The rate shall include making cutouts for tube lights, spot lights, duct doors, of specified size, grills etc. for which no extra cost shall be paid separately</p> <p>iii. Rate shall include providing additional trimming around cutouts for light fittings, cove lighting</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		arrangement and grills and providing additional supports from ceiling where main / cross members are cut for light fittings etc. No extra cost shall be paid for providing multilevel false ceiling, cove lighting arrangement etc. Note : Horizontal area only shall be measured for payment
11.	Acoustic Mineral Fibre False Ceiling	<p>i. Providing and fixing in true horizontal level false ceiling grid as approved by ASCL, using hot dipped galvanized steel section, exposed surface chemically cleaned capping prefinished in backed polyester paint, main tee of size 24x38x.33mm at every 600 c\c max and rotary stitched cross tee of size 24x30x.457mm wall around the wall to form Grid size of 600mmx600mm and suspending the grid using 2mm GI rod and 5mm Nylon rawl plug at every 1200 mm intervals at the main tee and laying mineral fiber Acoustic ceiling board of prima fine fissured type of size 600mm x 600mm x 15mm having fire rating of 60 minutes as per BS 476 /23 of 1987, Noise Reduction coefficient (NRC) of 0.50 to 0.55, sound Attenuation of 34 dB, Thermal conductivity of K = 0.052 w/m, weight of 3.5 kg / sq. meter and Humidity resistance greater than 90%</p> <p>ii. Rate shall include necessary wastage, clips, GI screws, etc. complete. Rate to include making necessary cut-outs or opening for light fixture etc., complete. The rate inclusive of labour &amp; material all complete</p>
12.	Flooring	<p>i. Providing and fixing Cavity floor systems of approved make as per site requirement and as per the following specifications System: Access floor system to be installed shall provide a maximum finished floor Height of 600mm from the existing floor level. The system shall provide for suitable pedestal and under-structure designed to withstand various static loads and rolling loads subjected to it in an office / server / DCS / panel / rack area. The entire Access floor system shall provide for adequate fire resistance, acoustic barrier and air leakage resistance.</p>
13.	Panels	<p>i. Panels shall be made from steel. The bottom of the panel shall be embossed in 49 hemispherical shape of 60mm dia and 12 reverse conical of 25mm dia to give strength and flexural rigidity. The top sheet shall be plain and resistant welded at various locations after the top and bottom sheets have been degreased and phosphated. The above hollow panel shall have an infill of light weight cementations material. The entire panel shall be coated with epoxy coating on the exposed surface. Panels shall remain flat through and</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>stable unaffected by humidity or fluctuation in temperature throughout its normal working life</p> <p>ii. Panels shall provide for impact resistance top surfaces minimal deflection, corrosion resistance properties and shall not be combustible or aid surface spread of flame. Panels shall be insulated against heat and noise transfer. Panels shall be 600mmx600mm fully interchangeable with each other within the range of a specified layout. Panels shall rest on the grid formed by the stringers which are bolted on to the pedestals. Panels shall be finished with anti-static Laminate of approved colour and PVC beading /trimming along the edges</p> <p>iii. The panel should be designed for a concentrated point load of 560 kg. and a uniformly distributed load (UDL) of 1800 kg/sq. meter The maximum permissible deflection should not exceed 2mm</p>
14.	Pedestals	<p>i. Pedestal installed to support the panel shall be suitable to achieve a finished floor height of 75 to 600mm. Pedestal design shall confirm speedy assembly and removal for relocation and maintenance. Pedestal base to be permanently secured to position on the subfloor. Pedestal assembly shall provide for easy adjustment of levelling and accurately align panels to ensure lateral restraint. Pedestals shall support an axial load of 2000 Kgs, without permanent deflection and an ultimate load of 3500 Kgs. Pedestal head shall be designed to avoid any rattle or squeaks</p>
15.	Pedestals Assembly	<p>i. Consisting of 100 x 100 x 2mm thick galvanized epoxy polyester coated MS Base plate die-pressed orbitally riveted to a 21mm. O.D. 2.5mm thick epoxy coated MS pipe to engage the pedestal head assembly. The pedestal head assembly consists of an embossed steel plate having 4 holes with <math>\frac{1}{4}</math> the tapping for fastening and locating of tile; orbitally riveted to a corresponding threaded stud 16mm dia. (O.D), length 100mm which is designed to engage the pedestal base assembly. The assembly shall provide a range of height adjustment upto 25mm, with the help of check nuts.</p>
16.	Under structure	<p>i. Under structure system consists of stringers of size 575 x 30x 20 x 1.5mm to form a grid of 600 x 600mm. These stringers are locked into the pedestal head and run both ways. The US system shall provide adequate solid, rigid and quiet support for access floor panels.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>ii. Uninterrupted height of 550 mm between the bottom of the floor and bottom of the access floor for electrical conducting and wiring Stringers: Stringer system is all steel construction, rectangular channels 30 x 20 x 1.6mm thick with pre-punched counter sunk holes at both ends for securing the stringers onto the pedestal head ensuring maximum lateral stability in all directions. The grid formed by the pedestal and stringer assembly shall receive the floor panel. Rate shall include preparation of surface, supply of Lifting hook - 2 Nos, cutting for supply/return Air Grills and for Grommet of required size, wastages, lead &amp; lift, grouting the system with anchor fastener, removing all debris from the premises etc. complete, as directed and for providing Class-'O' 19mm thick Nitrile rubber of approved make as a subfloor insulation fixed with approved non-formaldehyde based adhesive to the entire area of existing floor (Below false flooring) as per manufacturer's specification. Rate shall be inclusive of providing ramp and landing in the entry, finished with the antistatic laminate panel</p> <p>iii. Providing new flooring Floor tiles (seamless) conforming to ISO 13006/EN 176 Group Bias with technical specification as Mohs scratch hardness greater than 6, Water Absorption of 0.06%, Modulus of Rupture greater than 27 N/mm, Deep Abrasion resistance less than 204 mm cube, Surface flatness, Straightness of sides <math>\pm</math> 0.25%, thickness <math>\pm</math> 5% of size of approved colour and size &amp; thickness as specified below, set in 1:4 cement mortar over the existing sub-floor and pointing the joints with approved joint filler grout compound of matching shade as per Manufacturer's Specification and as directed. Rate shall include for wastages, for preparation of base surface, cleaning, acid wash, and protection of new finished floor with Gypsum / POP layer over Plastic sheet and removing the same before handing over, work at all levels and as directed. Rate shall be inclusive of wastages, etc. complete. Size of tiles shall be 600mm x 600mm and 10mm thick</p> <p>iv. Providing &amp; Fixing 2mm thick Anti-static vinyl flooring of approved make and shade finished flush with the Cavity Floor level</p> <p>v. Providing and Fixing Polypropylene Modular Carpet Tile flooring in the Meeting Room of approved make. It should conform to Loop Pile construction, min. total thickness of 6mm, and min. total pile weight of</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		20 oz./yd. Installation as per manufacturer's specifications, complete
17.	Joinery	<p>i. Providing and Fixing Style-less Glass Doors with Patch fittings made of 12mm thick toughened glass. Rate shall include all necessary hardware such as heavy duty floor spring, top pivot, floor-recessed locking arrangement, 450mm high S.S door handle of approved makes &amp; sample, etc. complete</p> <p>a) Single Door GD1 of size 900 x 2100 mm</p> <p>b) Double Door GD2 of size 1645 x 2100 mm</p> <p>ii. Providing and fixing 35 mm thick Flush Door shutters with 1.5mm tk. laminate finish single leaf of solid core of block board type bonded with phenol formaldehyde synthetic resin thermo pressed with 8 mm thick teak wood external lipping. The construction procedure of the shutter should be as per IS 2202. The shutter shall be shop prepared for taking mortice lock or latches suitable lock block of wood may be provided for fixing the hardware. The size of block, shall perfectly correspond to the maximum size of lock, covered in IS 2209. All the four edges of the door shutter shall be square.</p> <p>iii. The shutter shall be free from twist or warp in its plane and of required size etc.</p> <p>iv. Rate to include providing and fixing necessary lever handle with mortise lock, door closers, ball bearing hinges all of approved make. Rate also to include 200 x 600mm glass vision panel of 6mm thick with suitable wooden beading duly polished / painted</p> <p>a. Single Door D1 of size 900 x 2100 mm</p> <p>b. Single Door D2 of size 750 x 2100 mm</p> <p>v. H3 Providing and fixing of 2-hour rated Hollow metal fire door with Vision Panel of fully flush type of 46 mm thick, Pressed Galvanised steel Double leaf Guardian of approved make, which consists of frame, shutter, infill and finish as detailed below and conforming to IS:277</p> <p>vi. Door frame shall be double rebate profile of size 143 x 57 mm with bending radius of 1.4 mm having 1.6 mm thick galvanised steel sheet (16 gauge) with steel door shutter of 46 mm thick fully flush, double skin door shall manufactured from 1.25 mm thick galvanised steel sheet (18 gauge).The infill material shall be resin bonded honey comb paper with thermal insulation. Door frames and shutter shall be finished with etched primer coating, stored zinc phosphate primer and thermosetting synthetic enamel paint (35 micron DFT) of approved colour. The rate shall include for supply and fixing of 3 mm thick base</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>plates, all joints of frames with provision for anchor bolt fixing to wall / partition / RC surface, reinforcement pad for fixing of door closers of approved make, factory finish pre-punched cut outs to receive hardware and iron mongery, 3mm thick hinge plates predrilled to receive hinges for screw mounted fixing, stainless steel double bearing butt hinges of size 102 x 89 x 3 mm thick, mortice sash lock with 5 pin tubular brass cylinder 70 mm thick with internal thumb / knob operation and external key provision with knob, brass / nickel lever handles and heavy duty automatic door closer of approved make. Rate shall also include for grouting the frame with cement slurry including providing necessary Elastic fire stop Sealant at the Joints between Wall &amp; Frame to the required thickness and to be applied by using Dispenser tool CS 201 P1as per manufacture's specification etc. complete and as directed.</p> <p>vii. Rate shall be inclusive of providing and fixing Vision Panel of size 200 x 300mm of approved make fire rated glass of required thickness. Rate shall be inclusive of making cut-outs, provisions, etc. for receiving Access Control provision.</p> <ul style="list-style-type: none"> <li>a) Single Door FD1 of size 1200 x 2400 mm with Panic Bar</li> <li>b) Double Door FD2 of size 1500 x 2250 mm.</li> </ul> <p>viii. Rate shall include providing and fixing of plywood framework below Cavity floor to receive the Door floor spring, other hardware, etc. The plywood framework shall be properly anchored from the existing floor to ensure proper rigidity and avoid vibration during door movement. The plywood shall be finished with 2 coats of fire proof paint over a coat of anti-termite treatment / anti-corrosive primer to receive screws / anchor fasteners to fix Joinery frame in position etc. complete.</p> <ul style="list-style-type: none"> <li>a. Single Door FD3 of size 900 x 2100 mm</li> <li>b. Double Door FD4 of size 1800 x 2250 mm.</li> </ul> <p>ix. Rate shall include providing and fixing of plywood framework below Cavity floor to receive the Door floor spring, other hardware, etc. The plywood framework shall be properly anchored from the existing floor to ensure proper rigidity and avoid vibration during door movement. The plywood shall be finished with 2 coats of fire proof paint over a coat of anti-termite treatment / anti-corrosive primer to receive screws / anchor fasteners to fix Joinery frame in position etc. complete.</p> <ul style="list-style-type: none"> <li>a. Single Door FD5 of size 1200 x 2400 mm.</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>b. Double Door FD6 of size 2400 x 2400 mm.</p> <p>c. Double Door FD7 of size 1500 x 2400 mm.</p> <p>x. H4 Providing and Fixing 2 hour fire rated fixed glass with frame of Prompt or approved make. Rate shall include all hardware and assembly arrangements.</p>
18.	Painting Works	<p>i. Providing and applying two coats of Plastic emulsion paint to existing brick walls &amp; RC Columns of approved colour over a coat of water based primer including preparation of surface by thorough cleaning and wetting and applying POP / Gypsum powder putty as per manufacturer's specification fully to give an even shade before painting and curing as per manufacturers specifications and as directed. Paint to be applied with roller.</p> <p>ii. J2 Providing and applying good quality of ISO branded Plaster of Paris throughout the internal brick wall surface. POP punning thickness should be 12mm &amp; above across all the internal surface and finished to uniform smooth finish.</p>
19.	Miscellaneous Works	<p>i. Making of openings in existing brick wall for Electrical / AC services connections and filling up the same with brick bats in 1:5 cement mortar mixed with waterproofing compound to finish flush with adjacent wall surfaces and matching wall thickness.</p> <p>ii. Sealing of all penetrations through the Data centre area to allow services routing, etc. by using fire resistant bulk-head sealant of quality makes. Complete and tested as per manufacturer's specifications</p> <p>iii. Chipping of existing sub-flooring to a required width and depth for floor trunking, raceways, junction boxes and conduits, and redoing / re-finishing the same with C.C 1:2:4 to make good the surface</p> <p>iv. Chasing in existing brick walls to accommodate concealed conduits &amp; pipes to required width and depth as per Electrical &amp; AC requirements, and refilling the same with 1:4 cement plaster to finish flush with adjoining surfaces</p> <p>v. Providing and Fixing S.S Handrail for Data centre access ramp along the 115mm brick wall made of 50mm dia. SS pipe with necessary intermediate wall support of 32mm dia. S.S pipe grouted in existing brick wall and welded to the 50mm dia. Pipe. The main handrail pipe shall be fixed 2" away from the wall / intermediate column and shall follow the slope of the ramp. The installation should have sufficient rigidity and welded joints should be neatly levelled and finished.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>vi. Providing and placing 300 x 300 x 300 mm high concrete pedestals at Ground floor to mount the Electrical panels and other equipment.</p>
20.	General Requirements	<p>i. All requirements such as skilled and unskilled labour, plant, equipment, scaffolding, materials, etc. required for complete execution of the work in accordance with the drawings and as described herein and/or as directed by the ASCL/Consultant have to be met. All workmanship shall be in accordance with the latest standards and best possible practice. Masonry work shall be true to line &amp; level as shown on drawings. All such masonry shall be tightly built against structural members and bonded with dowels, anchors, inserts, etc., as shown on the drawings.</p>
21.	Materials Bricks	<p>i. Burnt clay bricks, for general masonry work, shall conform to IS: 1077 and for face brick work, shall conform to IS: 2691. First class quality table moulded chamber burnt bricks of nominal size 8-3/4" x 4-1/2" x 2-3/4" shall be used for general masonry work. Table moulded bricks should be used if manufactured locally.</p> <p>ii. Bricks for general masonry work shall be sound, hard, well burnt (but not over burnt) without being vitrified, of uniform size, shape, having sharp edges, cherry red colour and homogenous in texture. These shall be free from cracks, flaws or nodules of free lime and shall emit clear ringing sound (metallic sound) when struck. These shall not show any signs of efflorescence either when dry or subsequent to soaking in water. Fractured surface shall show uniform texture free from girts, lumps, holes etc.</p> <p>iii. Unless otherwise specified, minimum compressive strength shall correspond to class designation 50 as per IS: 1077 with a minimum crushing strength of 50 kg/sq.cm. For general masonry work, Water absorption after 24 hours immersion shall not exceed 20% by weight for common bricks and 15% for face bricks.</p> <p>iv. Bricks shall be stacked on dry firm ground in regular tiers even as they are unloaded to minimize breakage and defacement of bricks. Bricks of different class, selected for various categories of use in the work, shall be stacked separately. Each stack shall contain equal number of bricks, preferably not more than 3000.</p> <p>v. Representative samples of bricks shall be submitted to the Consultant for approval before supply to site and the approved samples shall remain with the</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		ASCL. All bricks proposed to be used shall conform to the approved samples in all respects. Bricks picked up at random from the stacks shall be tested as to ascertain to satisfy the acceptability requirements as and when desired by the Consultant at the MSI's cost
22.	Cements	<ul style="list-style-type: none"> <li>i. The cement used shall be the Ordinary Portland cement conforming to IS: 269 and IS: 8112. Unless otherwise specified ordinary Portland cement of 43 grade conforming to latest IS - 8112 shall be used for all masonry and concrete works.</li> <li>ii. Own arrangements for the storage of adequate quantity of cement should be made. Cement shall be stored in closed weather proof sheds with raised wooden plank flooring to prevent deterioration by damages or intrusion of foreign matter away from walls</li> </ul>
23.	Sands	<ul style="list-style-type: none"> <li>i. Sand shall conform to IS: 383 and IS: 2116. Sand shall have fineness modulus between 2.1 and 2.5. Sand shall be hard, durable, clear and free from dirt clay organic method or other impurities. Silt content of sand shall not exceed 5% by volume. Sand containing any trace of salt shall be rejected.</li> </ul>
24.	Water	<ul style="list-style-type: none"> <li>i. Water used for mortar and curing shall be clean and free from injurious amounts of deleterious matter such as oils, acids, alkalis, sugar, organic materials etc. Potable water is generally considered satisfactory for mixing masonry.</li> </ul>
25.	Lime	<ul style="list-style-type: none"> <li>i. Lime shall be stone lime and it shall conform to IS: 712. Hydrated lime shall be mixed with water to form putty. This shall be stored with reasonable care to prevent evaporation of water for at least 24 hours before use. Quick lime shall be slaked with enough water to make a cream and then stored with reasonable care to prevent evaporation of water for at least seven days before use.</li> </ul>
26.	Scaffolding	<ul style="list-style-type: none"> <li>i. Unless otherwise instructed by the ASCL/Consultant, double scaffolding having two sets of vertical supports shall be provided for all building work. The supports shall be sound, strong and tied together with horizontal pieces over which scaffolding planks shall be fixed. The MSI shall be responsible for providing and maintaining sufficiently strong scaffolding so as to withstand all loads likely to come upon it.</li> </ul>
27.	Mortar	<ul style="list-style-type: none"> <li>i. IS: 2250 shall be followed as general guidance for preparation and use of mortar. Mixing of mortar shall be done in a mechanical mixer. Cement and sand shall be mixed dry in specified proportions thoroughly and then water shall be added gradually. Wet mixing shall</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>be continued till mortar of the consistency of a stiff paste and uniform colour is obtained. Only the quantity of mortar which can be used within thirty minutes of its mixing shall be prepared at a time. Hand mixing may be allowed by the ASCL on clean approved platform in special cases only.</p> <p>ii. Mortar shall be used as soon as possible after mixing and before it has begun to set and in any case within thirty minutes after the water is added to the dry mixture. Mortar left unused for more than thirty minutes after mixing shall be rejected and removed from the site of work. Surplus mortar droppings while laying masonry, if received on a surface free from dirt, may be mixed with fresh mortar if permitted by the ASCL, where directed for addition of extra cement and this shall be implemented.</p>
28.	Brick Masonry	<p>i. Only cement-sand mortar shall be used. Unless otherwise specified, mortar for brickwork having one or more brick thickness shall be 1 part cement and 6 parts sand by volume as specified. Mortar for half-brick thick walls shall be 1 part cement and 4 parts sand by volume. Richer mix proportion shall be used, whenever specified or as per design requirement. Mortar shall meet the compressive strength requirement as per IS:2250 and IS:1905</p>
29.	Laying of Bricks	<p>i. IS: 2212 shall be followed as general guidance for construction of brick masonry. Bricks shall be soaked in water before use for a period generally not less than 6 hours so that the water just penetrates the whole depth of the bricks.</p> <p>ii. Bricks shall be laid in English Bond unless otherwise specified. Half or cut bricks shall not be used except where necessary to complete the bond. Closer in such cases shall be cut to the required size and used near the ends of the walls, next to quoin headers.</p> <p>iii. Bricks shall be laid generally with frogs upwards. A layer of mortar shall be spread on the full width and over a suitable length of the lower course. Each brick shall be properly bedded and set home (in position) by gently tapping with the trowel handle or with a wooden mallet. Its inside face shall be buttered with mortar before the next brick is laid and pressed against it. On completion of a course, all vertical joints shall be fully filled from the top with mortar. The thickness of joints shall be kept uniform and shall not exceed 10 mm. Bricks shall be so laid that all joints are full of mortar.</p> <p>iv. All face joints shall be raked to a minimum depth of 15 mm by raking tools during the progress of</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>brickwork, when the mortar is still green, so as to provide proper key for the plaster or pointing to be done. When plastering or pointing is not required to be done, the joints shall be struck flush and finished at the time of laying.</p> <ul style="list-style-type: none"> <li>v. Brickwork in walls shall be taken up truly plumb. All courses shall normally be laid truly horizontal unless indicated to be laid on slope and all vertical joints shall be truly vertical. Vertical joints in alternate courses shall come directly one over the other. Brick wall shall be construed with at least one plain face with proper alignment.</li> <li>vi. All connected brickwork shall be carried up simultaneously and no portion of work shall be left more than one meter below the rest of the work. Where this is not possible, in the opinion of the ASCL, the work shall be raked back according to bond (and not toothed) at an angle not steeper than 45 deg. The work done per day should not be more than one meter height All iron fixtures, pipes, water outlets, hold fasts for doors and windows, etc. which are required to be built into the brickwork shall be embedded in their correct position in mortar or cement concrete as the work proceeds as per directions of the ASCL/Consultant.</li> <li>vii. All brickwork shall be built tightly against columns, floor slabs or other structural parts and around door and window frames with proper distance to permit caulked joint. Wherever deemed necessary structural steel columns and spandrel beams are to be partly or wholly covered with brickwork, the bricks shall be laid closely against all flanges and webs with all spaces between the steel and brickwork filled solid with mortar not less than 10mm in thickness.</li> <li>viii. The top courses of all plinth, parapet, steps and top wall shall be laid with brick on edge unless otherwise specified. Care shall be taken that the bricks forming the top courses and ends of walls are properly radiated and keyed into position.</li> <li>ix. Scaffolding shall be strong enough to withstand all the dead, live and impact loads which are likely to come upon it. It shall also be so designed as to ensure the safety of the workmen using them.</li> <li>x. In case of joining old brickwork with new brick work, the old work shall be toothed to the full width of the new wall and to the depth of quarter of a brick in alternate courses. It shall be cleaned of all dust, loose mortar, etc., and thoroughly wetted before starting new brick work. Thickness of each course of new work</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>shall be made equal to the thickness of the corresponding course of the old work by adjusting thickness of horizontal mortar joints.</p> <p>xi. The face of the brickwork shall be cleaned on the same day on which brickwork is laid and all mortar dropping removed promptly.</p> <p>xii. Template (bed-block) of plain or reinforced cement concrete shall generally be provided to support ends of RCC beams. Top surface of the wall shall be suitably treated as per direction of the ASCL/Consultant so as to minimize the friction to movement of the concrete slab over the bearing.</p> <p>xiii. Brickwork shall be protected from rain by suitable covering when the mortar is green. Masonry work shall be cured by keeping it constantly moist on all faces for a minimum period of seven days. Brickwork carried out during the day shall be suitably marked indicating the date on which the work is done so as to keep a watch on the curing period.</p>
30.	Half brick masonry	The work shall be done in the same manner, as mentioned in 7.02 except that all courses shall be laid with stretchers. Unless otherwise specified the walls with RCC (1:2:4) binders reinforced with 2 nos. of 8 mm mild steel bars and 6 mm MS tie bars at 230 intervals. The cost of half brick work shall include the cost of reinforcement and form work for binders. RCC band shall be of size 115 mm wide x 80 mm high and shall be continuous, unless where broken by openings in walls.
31.	Exposed brickwork	<p>i. Exposed brickwork i.e. brickwork is superstructure which is not covered by plaster shall be done by especially skilled masons. All courses shall be laid truly horizontal and all vertical joints shall be truly vertical. Vertical joints in alternate courses shall come directly one over the other.</p> <p>ii. Thickness of brick courses shall be kept uniform and for this purpose wooden straight edge with graduations indicating thickness of each course including joint shall be used. The height of window sills, bottom of lintels and other such important points in the height of the wall shall be marked on the graduated straight edge. Masons must check workmanship frequently with plumb, spirit level, rule and string.</p> <p>iii. For all exposed brick work, double scaffolding having two sets of vertical supports shall be provided. The supports shall be sound and strong, tied together with horizontal pieces over which scaffolding planks shall be fixed.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>iv. If face bricks shall be in composite work with face bricks on the exposed face and balance in standard bricks, but maintaining the bond fully. Where face bricks are not specified, bricks for the exposed face shall be specially selected from available stack of bricks. All exposed brickwork on completion of work shall be rubbed down, washed clean and pointed as specified. Where face bricks are used, carborundum stone shall be used for rubbing down</p>
32.	Reinforcing anchorage	For external walls, the anchorage in the form of flats or rods from spandrel beams and columns and any other anchoring and reinforcement shall be adequately embedded in the masonry
33.	Mode of measurement	<p>i. Unless noted otherwise in the bill of quantities, the method of measurement for various items shall be generally in accordance with IS 1200, subject to the following.</p> <p>ii. Except where otherwise described, stone work and stone walling general shall be given in cubic meters and fascia work in square meters.</p> <p>iii. When measuring walls, the thickness shall be measured to the nearest one centimetre. Deductions shall be made as described in IS: 1200.</p>
34.	Materials	<p>i. Materials shall be of the best approved quality obtainable and they shall comply with the respective Indian Standards Specification.</p> <p>ii. Samples of all materials shall be got approved before placing order and the approved sample shall be deposited with the ASCL</p> <p>iii. In case of non-availability of materials in metric sizes, the nearest size in FPS units shall be provided with the prior approval of the ASCL/Consultant for which no extra cost shall be paid nor shall any rebate be recovered.</p> <p>iv. If directed, materials shall be tested in any approved Testing Laboratory and the Test Certificate in original shall be submitted to the ASCL and the entire charges of testing including charges for repeated tests if ordered shall be borne by the Contractor.</p> <p>v. It shall be obligatory for the MSI to furnish Certificate, if demanded by the ASCL/Consultant, from manufacturer or the material supplier that the work has been carried out by using their material and as per their recommendation.</p> <p>vi. All materials supplied by the ASCL or any other government departments directed by the ASCL shall be properly stored and the MSI shall be responsible for its safe custody until they are required on the works and till the completion of work.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>vii. Unless otherwise mentioned in the Schedule of Quantities or Special Specifications the quality of materials, workmanship, dimensions, etc. shall be as specified here-in-under.</p> <p>viii. All Equipment and facilities for carrying out field tests on materials shall be provided without any extra cost</p>
35.	Mode Measurements of	<p>i. Doors, Windows and Grills Clear area over one face inclusive of frame shall be measured. Hold fasts and portions embedded in masonry or flooring shall not be measured.</p> <p>ii. Internal Partitions (Gypboard, Plywood, etc.) The partition height shall be measured upto bottom of false ceiling and framing members / ply / Gypboard going above shall not be measured.</p> <p>iii. Decorative panelling over wall or over partitions the area of cladding shall be measured in square metre, or square feet. The gross area cladded shall be measured. No deductions shall be made for gaps upto one centimetre between the panels.</p> <p>iv. Vitrified Ceramic Tile: the actual area covered by the vitrified tile shall be measured. No extra shall be allowed for wastage.</p> <p>v. Paving and tile work the work mentioned in this section shall be measured in Sq. ft. /Sq. meter and shall be priced per unit of Sq. ft. / Sq. meter In all paving work, the slabs shall be touching the walls and go well under the plaster, but the measurements shall be the clear measurements of the rooms or areas when finished. No allowance shall be made for portions going under the plaster.</p> <p>vi. False ceiling: For false ceiling work, the measurement shall be for the actual area covered. No deductions shall be made for the cut-outs, for light fittings, speakers, column upto 5.00 Sq.ft. / 0.50 Sq. meter.</p> <p>vii. Wood work: For conversion of inches to feet/cm to metre, the resultant figure shall be taken upto two digits after decimal point. Third digit shall not be taken into account.</p> <p>viii. Note: All materials shall be of the 1st quality and ISI marked. Wherever MSI shall use standard product makes which shall be approved ASCL/Consultant. Any additional expenditure and time due to this shall be solely on MSI's account and no claims whatsoever shall be entertained, in this regard.</p>

### 6.7.7 Non IT – Electrical Cabling: Guidelines and Specifications

S. No.	Nature of Requirement	Guidelines / Specifications
1.	Raw Power	<ul style="list-style-type: none"> <li>i. Power supply from two different substation to be ensured for redundancy. Appropriately Substation to be commissioned and automatic fail over of substations to be enabled. The power distribution room is tentatively planned to commission in BASEMENT of the Municipal corporation office</li> <li>ii. Power from the Main Panel (Dual Line) shall be received in a Main MV Panel of Single busbar type to be located at Electrical Panel at Basement</li> <li>iii. Electrical Panel for Raw power to ICCC, DC &amp; UPS in Second floor shall be planned in Basement</li> <li>iv. Electrical Panel for DG to ICCC, DC &amp; UPS in second floor shall be planned in Basement</li> <li>v. All interlocking arrangement shall be done thro' Electrical / Mechanical interlocking arrangements</li> <li>vi. From this panel, feeders can be taken to various requirements as under:- Sub Power Panel for Raw Power and AC distribution. <ul style="list-style-type: none"> <li>a. Incoming of 250KVA UPS - 1</li> <li>b. Incoming of 250KVA UPS - 2</li> <li>c. Incoming of 20KVA UPS -1</li> <li>d. Incoming of 20KVA UPS - 2</li> </ul> </li> <li>vii. Two Numbers of 630KVA DG sets has been proposed to be installed in the Basement with Auto Synchronising panel</li> <li>viii. Moulded Case Circuit Breakers along with Air Circuit Breakers shall be used in the construction of distribution panels. The final distribution shall be done using Miniature Circuit Breakers. All underground cables are of XLPE sheathed Aluminium cable for the rating above 25 Sq.mm. PVC sheathed Aluminium cable for the rating below 25 Sq.mm. The Panels shall have MCCBs as components and not FSUs. The panels / switch boards shall have sufficient spares as required to provide for future additions or alterations. From the Main panels, Underground PVC insulated XLPE sheathed cables shall be used to transmit power to the Main Building and Guest Block. The cables shall be laid in the bare ground with necessary bricks, sand layers and with Cable Route Markers (or) in a permanent constructed trench with precast slab as cover</li> <li>ix. The final distribution boards (LDBs and PDBs) which feed the socket outlets, lighting circuits and other requirements are protected by ELMCBs which in turn protect the downstream circuits too</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>x. From the final distribution boards, copper cabling shall be laid above false ceiling shall be enclosed in MS conduits as a safety measure against spread of fire in case of some accident. MS conduits shall be used in case of concealed wiring</p>
2.	Cables and Terminations	<p>Cables</p> <p>i. All Power cables shall be of aluminium / copper conductors only. All control cables shall be of solid or stranded copper conductors. The control cables used for mobile equipment shall be flexible type. Power cables for 415 V AC and upto 1000 V DC and control cables for wiring within the building shall be of PVC insulated and PVC sheathed armoured / unarmoured heavy duty 1100 V grade. Cross-sectional areas of multi core power cables shall not exceed 400 sq.mm unless otherwise specified. Minimum cross-sectional area of power cable shall be 6 sq.mm in case of aluminium conductor and 1.5 Sq.mm in case of copper conductor. The cross-sectional area of neutral conductor of multicore cables shall constitute about 50% of phase conductor for cables having cross-sectional are of 25 sq.mm and above. However this is not applicable for UPS distribution. For cables below 25 sq.mm as well as flexible trailing cables, the neutral conductor shall be of same cross-section area as the phase conductor. All cables 10 sq.mm and above shall be of stranded type.</p> <p>ii. PVC Cables: PVC insulated, XLPE Sheathed / PVC sheathed armoured/unarmoured heavy duty cable shall be designed, manufactured and tested in accordance with IS : 1554 (PART - I). The insulation shall consist of polyvinyl chloride compound suitably extruded with softeners and plasticizers. The inner sheath shall be either vulcanized rubber or PVC. The outer sheath shall be of XLPE compound. The armouring of multi-core cables where required shall be of single layer galvanized steel round wire or flat strip.</p>
3.	Cable Selection	<p>i. The power cable sizes shall be adopted on the basis of current loading, ambient temperature condition, method of installation and permissible voltage drop in each circuit. The minimum cross-section of the cable shall be determined on the basis of available short circuit current and tripping characteristics of the circuit protective devices. Colour code shall be maintained for the entire wiring installation (i.e.) Red, Yellow and Blue for the three phases, Black for neutral and Green for earthing. Besides, ferruling shall be provided with number coding and easy identification for maintenance purposes.</p>
4.	Cable Joining	<p>i. Cable jointing shall be done as per the recommendations of the cable manufacturer. Jointing shall be done by</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		qualified cable jointers. Each terminations shall be carried out using brass compression glands and cable sockets. Hydraulic crimping tool shall be used for making the end terminations. Cable gland shall be bonded to the earth by using suitable GI Wire / tape. Suitable identification tags with the feeder designation inscribed on an aluminium / G.I. Sheet steel be tied to either ends of each cable
5.	Cable Conduit trays	<ul style="list-style-type: none"> <li>i. Cables shall be laid on cable trays/ racks wherever specified. Cable racks/ trays shall be of perforated steel section slotted angles for suitable purpose. The trays / racks shall be complete with plates, tees elbows, risers and all necessary hardware. The steel trays shall be painted. Cable trays shall be erected properly to present a neat and clean appearance. Suitable cleats or saddles shall be used for securing the cables to the cable trays. The cable trays shall comply with the following requirements:-</li> <li>ii. The trays are ladder type and shall have suitable strength and rigidity to provide adequate support for all contained cables</li> <li>iii. It shall not present sharp edges, burrs or projections injurious to the insulation of the wiring / cables</li> <li>iv. If made of Sheet metal, it shall be adequately strength protected against corrosion or shall be made of corrosion resistant material</li> <li>v. It shall have side rails or equivalent structural members</li> <li>vi. It shall include fittings such as horizontal, vertical bends, tie rods, hooks etc., or other suitable means for changes in direction and elevation of runs, fish plates and hard wire</li> </ul>
6.	Cable support systems	<p>Method of Laying Cables:</p> <ul style="list-style-type: none"> <li>i. Cables laid exposed in racks/trays/hooks and routed from trenches to individual equipment etc. shall be taken in embedded / exposed rigid G.I pipes or flexible conduits unless directly terminated to the equipment in the panels located above the trench. Extra length of cables shall be provided wherever possible for any future contingency to the extent of 10% of the length of any section. The cables laid fully buried in ground or partly in trench and partly in ground shall be armoured type. Cables are laid fully in rack/tray/hook or laid in G.I. pipes, shall be also armoured type.</li> <li>ii. The installation work shall be carried out in a neat workman like manner by skilled, experienced and competent workmen particularly with experience in jointing termination of aluminium conductor cables. Cables runs shall be uniformly spaced properly supported and protected in an approved manner. All</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		bends in runs shall be well defined and made with due consideration to avoid sharp bending and linking of the cable. The minimum bending radius of cables shall not be less than twelve times the overall diameter. Cable installation shall be property co-ordinates at site with the routing of other services, utilities and the cable routings with a view to avoid interference with any part of the building, structure, equipment, utilities and services. All cables shall be provided with identification tags indicating the cable numbers in accordance with the cable/circuit schedule. Tags shall be fixed at both the ends of cable at joints and at 20 m spacing for straight runs. When a cable passes through a wall tags shall be of durable fibre of aluminium sheet with the numbers punched on them, and securely attached to the cables with non-corrosive wire. For single core cables wire shall be non-ferrous material. All cables shall be tested for proper insulation prior to laying. The cable drums shall be transported on wheels to the place of work. The cables shall be laid out in proper direction as indicated on the drum using cable drum stands. In case of higher size cables, the laid out cables shall run over rollers placed at close intervals and finally transferred carefully on to the trenches and racks. Care shall be taken so that links and twists or any mechanical damage does not occur in cables. Only approved cable pulling grips or other devices shall be used. Adequate length of cables shall be pulled inside the switchboards, control panels, terminal boxes etc. so as to permit neat termination of each core/conductor. Control cables cores entering switchboard or control panels shall be neatly bunched and strapped with PVC perforated tapes and suitably supported to keep it in position at the terminal block. All spare cores shall be neatly dressed and suitably taped at both ends. Power cable terminations shall be carried out in such a manner to avoid strain on the terminals by providing suitable clamp near the terminals. All power cable terminations shall be by means of crimping type cable lugs. Control cables shall be terminated by crimping or directly clamped in the terminal blocks by screws. No jointing shall normally be made at any intermediate point in through runs of cables unless the length of the run is more than the length of the standard drum supplied by cable manufacturers. In such cases when jointing is unavoidable, the same shall be made by means of standard cable jointing boxes/kits. All cables entry openings in the equipment shall be sealed and made proof against entry of creeping reptiles.

S. No.	Nature of Requirement	Guidelines / Specifications
7.	Laying of Cables on Racks / Trays / Brackets	<p>i. Power cables in trenches and on structures shall be laid on racks and shall be clamped by means of single or multiple galvanized MS saddles. The saddles shall be placed at an interval of 1000 mm. in both horizontal and vertical straight runs, at each bend and turnings from horizontal to vertical direction and vice versa. All 1100 V grade power cables shall be laid touching each other. Multi-core control cables shall be laid touching each other on trays and wherever required may be taken in two layers. G I Ladder type cable racks shall be selected from two sizes viz.</p> <p>ii. 600 mm. and 1500 mm. Ladder type trays shall be galvanized after fabrication. And inside the module shop only G I perforated type cable trays shall be used. Vertical spacing between cable racks/trays shall be 250 mm. Power cables of different voltage grades shall be laid in separate racks / brackets / hooks. Control cables as well as signal and communication cables shall be laid in a separate trays. However, in cases where smaller size power cables (below 16 sq.mm.) of fewer numbers cables provided suitable vertical barriers are installed between them. As far as possible AC and DC Power cables shall be laid in separate trays. Order of laying of various cables in racks/trays brackets/hooks shall be such that control cables are located at the bottommost tier and 1100 V grade cables at top tier. In case of duplicate feeders of same consumer, these shall be laid in two separate racks/brackets. Where there is possibility of mechanical damage, cable rack / trays shall be adequately protected by sheet steel covers. For future installation of cables, provision shall be made to keep 20% space as spare on each ray/rack/bracket.</p>
8.	Cables In Indoor Trenches	<p>i. Cables shall be laid in indoor trenches wherever specified. Suitable angle iron brackets, clamps, hoods and saddles shall be used for securing the cable in position.</p>
9.	Cables On Trays / Racks	<p>i. Cables shall be laid on cable trays/ racks wherever specified. Cable racks/ trays shall be of perforated steel section slotted angles for suitable purpose. The trays / racks shall be complete with plates, tees elbows, risers and all necessary hardware. The steel trays shall be painted. Cable trays shall be erected properly to present a neat and clean appearance. Suitable cleats or saddles shall be used for securing the cables to the cable trays. The cable trays shall comply with the following requirements:-</p> <p>ii. The trays are ladder type and shall have suitable strength and rigidity to provide adequate support for all contained cables.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<ul style="list-style-type: none"> <li>iii. It shall not present sharp edges, burrs or projections injurious to the insulation of the wiring / cables.</li> <li>iv. If made of Sheet metal, it shall be adequately strength protected against corrosion or shall be made of corrosion resistant material.</li> <li>v. It shall have side rails or equivalent structural members.</li> <li>vi. It shall include fittings such as horizontal, vertical bends, tie rods, hooks etc., or other suitable means for changes in direction and elevation of runs, fish plates and hard wire.</li> <li>vii.</li> </ul>
10.	Installation	<p>Installation</p> <ul style="list-style-type: none"> <li>i. Cable trays shall be installed as a complete system. Trays shall be supported properly from the building structure. The entire cable tray system shall be rigid.</li> <li>ii. Each run of the cable tray shall be completed before the installation of cables. Portions where additional protection is required, non-combustible covers / enclosure shall be used.</li> <li>iii. Cable trays shall be exposed and accessible.</li> <li>iv. Where cables of different system are installed on the same cable tray, non-combustible solid barriers shall be used for segregating the cables.</li> <li>v. Cable trays shall be grounded by two nos. earth continuity wires. Cable trays shall not use as equipment grounding conductors.</li> </ul>
11.	Installation of wiring conductors	<ul style="list-style-type: none"> <li>i. System of wiring</li> <li>ii. The system of wiring shall consist of FRLS flexible copper cables (or) PVC insulated PVC sheathed FRLS copper conductor wires in M S conduits. Minimum size of copper conductor shall be 1.5 sq.mm. For lighting and 4 sq.mm. For power. Colour code shall be maintained for the entire wiring installation (i.e.) Red, Yellow and Blue for the three phases, Black for neutral and Green for earthing. Besides, ferruling shall be provided with number coding and easy identification for maintenance purposes. M S conduits shall be used if they are concealed in the wall / slab.</li> </ul> <p>The following cable sizes shall be used in the installation:-</p> <ul style="list-style-type: none"> <li>a) Lighting circuits: 2.5 Sq.mm.copper</li> <li>b) Point Wiring: 1.5 Sq.mm.Copper</li> <li>c) Power Circuits (16 Amps): 4.0 Sq.mm.copper</li> <li>d) Incomer to single phase LDB: 3 core 4.0 Sq.mm. copper</li> <li>e) Incomer to Three phase LDB: 4 c 10 Sq.mm. Aluminium</li> <li>f) Incomer to PDBs: 16.0 Sq.mm. Aluminium to 25.0 Sq.mm. Aluminium depending on requirement.</li> <li>g) UPS Circuit (server room): 3 core 4 Sq. mm flexible copper wire in MS conduit</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
12.	Wiring to walls and above false ceiling.	<p>h) UPS Circuit (workstation room): 3 runs 2.5 Sq. mm copper wire in MS conduit</p> <p>i. All wiring shall be carried out only with M S conduits all light, fan sockets and any other equipment must be earthed. Wiring shall be carried out with 650 V grade PVC insulated single core multi stranded copper conductor wires as per IS: 694. The method of wiring shall be as recommended in IS: 732 and its several parts. The physical and electrical continuity of the conduit system shall be maintained throughout. No wire shall be left exposed at any location; metallic flexible pipe shall be used to cover the same. Colour coding of wire shall be carried out as detailed below:</p> <ul style="list-style-type: none"> <li>a. PHASES RED/YELLOW/BLUE</li> <li>b. NEUTRAL BLACK (OR) GREY</li> <li>c. EARTH GREEN</li> </ul> <p>ii. The minimum diameter of the conduits shall be 25 mm. only. The following sizes of PVC insulated multi stranded copper conductor wires shall generally be followed throughout:</p> <ul style="list-style-type: none"> <li>iii. From the final switch to individual outlets 1.5 sq.mm</li> <li>iv. From Distribution Boards to First Switch Board and 2.5 sq.mm</li> <li>v. Subsequent switchboards all 15A socket (Only Phase &amp; Neutral) 4.0 Sq.mm.</li> <li>vi. Earth wire throughout for Lighting. 1.5 Sq.mm.</li> <li>vii. Earth wire for raw power 2.5 Sq.mm</li> </ul>

#### 6.7.8 Non IT – Earthing Network: Guidelines and Specifications

S. No.	Nature of Requirement	Guidelines / Specifications
1.	General Earthing System	<p>i. Distributed earthing shall be carried all along the LT distribution system, through local earth stations effectively bonding the cables / equipment.</p> <p>ii. For Main building, Substation and Electrical Panel DC Room, one main earthing ring shall be provided along the building periphery connected to required number of earth electrodes. The earthing ring shall be taken 1525 mm away from building column / wall and shall be laid directly buried in ground. Main earthing ring shall be further cross-connected and a mesh formed depending on the layout and location of the equipment. The cross-connections shall generally run in cable trenches, or embedded in concrete floor based on the layout.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>iii. All non-current carrying metallic parts of various electrical equipment as well as cable armouring metallic conduit/GI pipe system, cable racks/trays brackets, supporting structures etc. shall be effectively earthed. Earthing of medium and high voltage equipment shall be done by means of two separate earth conductors connected either directly to earth electrodes or to an earthing ring irrespective of use of armoured cable or metallic conduit/GI pipe.</p> <p>iv. Building / technological steel structures, metallic utility pipes shall not be used as earth continuity conductor. All earthing system shall be so designed as to ensure effective operation of protective gears in case of earth faults. The total earth resistance at any point of the earthing system for substations and main plant buildings shall not be more than one ohm. However, at other points the value shall not exceed 3.Ohms.</p> <p>v. Generally, main earthing rings and earthing leads shall be directly buried in ground. Additional earthing rings wherever provided inside plant buildings/substations and earth continuity conductors shall be taken either exposed on cable racks/trays, structures, walls, ceiling etc. or embedded in concrete depending on installation. Earth conductor directly buried shall be taken at a depth of 600mm. It shall be provided with one coat of bituminised paint, at all welded joints to prevent corrosion. Earthing ring wherever embedded in concrete shall be laid parallel to the column rows of buildings. Earth continuity conductor embedded in concrete shall generally follow the shortest route and wherever possible shall be taken along pipes embedded for laying of cables. Earth conductors lay on cable racks, trays etc. shall be placed in accessible location keeping adequate clearance to facilitate easy connections.</p> <p>vi. All 3 phase equipment shall have duplex earthing, whereas single phase equipment shall have only one run. Earthing for light and power points shall be carried out using insulated copper earth wire running throughout the length of circuits and shall be terminated at boxes, fixtures etc. with effective bonding to main earth.</p> <p>vii. Separate and distinct earth stations and electrodes shall be provided for UPS System, EPABX and Server Racks. Earthing for UPS Neutral, Server Racks and EPABX points shall be carried out with insulated copper earth wires. The total earth resistance at any point shall not be more than 1.Ohm</p>

S. No.	Nature of Requirement	Guidelines / Specifications
2.	Precautions	i. All jointing of earth flats shall be done in such a way that all surfaces shall be thoroughly cleaned and rubbed with emery paper before jointing. Ensure that there is no air gap between the flats after jointing.
3.	Safety Equipment's	i. All safety equipment's shall be positioned optimally as well as the procedures followed by the local authorities. All safety equipment's shall be as per IS standards as specified in the BOQ
4.	Fabricated type supports and Miscellaneous	i. Wherever needed, these supports shall be provided to suit the requirements. All supports shall be painted as specified. All supports shall be properly fixed on to the ceiling with necessary anchor fasteners.
5.	light Fittings fixtures work	i. The adequate Light fittings shall be deployed in the DC. The light fittings shall be preassembled with necessary ballasts, lamp holders, lamps, interconnections, terminal connectors and other associated accessories. The light fittings shall be carefully installed at site. Until hand over necessary protection sheets like polythene covers shall be provided so that no insects can go in.
6.	Electro Static Discharge (ESD) Control	i. The Data Centre shall be provided with appropriate methods & equipment to effectively reduce ESD. It is required that the personnel handling sensitive equipment shall use wrist straps, heel rounders etc. to reduce the likelihood of human instigation of ESD. Cabinets, Racks, cages shall be properly grounded & operated by trained officials during inspection, maintenance and repairs. Usage of room ionisers is preferred to attract charged objects for neutralization
7.	Emergency Power Supply	<p>i. Emergency supply system with Inverters shall be provided to maintain minimal light levels through an independent inverter system with Sealed. Maintenance Free batteries. Emergency lighting fixtures shall be located strategically. MSI should provision for Backup Diesel Generators sets to support the UPS in providing emergency power supply to the computer equipment in a prolonged power outage. The need of diesel generator depends on the service requirements of the computer system. However, the generator should also be able to support other essential facilities and equipment such as the air conditioning. System, security and access control system and lighting. The DG set shall come online automatically within 10 seconds of AC mains failure.</p> <p>ii. The DG set should have an Auto Synchronizing Panel (ASP) MV panel controller between main power &amp; DG set. MSI should make an arrangement with a Fuel Supply Company for continuous supply of Diesel to DG sets in case the Fuel supply is erratic, not available or is deficient on any reason whatsoever. The MSI should store diesel</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		sufficient enough to last for a minimum of 7 days. MSI shall provide the details and formal arrangement copy with the Fuel Company to ensure that MSI is guaranteeing fuel availability. MSI shall also provide the diesel storage and replenishment policy to ASCL. ASCL shall provide space for parking their Fuel Replenishment vans etc.
8.	Energy Saving	<ul style="list-style-type: none"> <li>i. Apart from implementing effective maintenance &amp; service schedules and use of energy efficient drives, especially motors, the following is proposed for implementation           <ul style="list-style-type: none"> <li>a. Use of LED indicators in EXIT signs with battery backup instead of incandescent lamps</li> <li>b. Use of energy efficient transformer</li> <li>c. Use of CFL lamps which are more efficient</li> <li>d. The LT side voltage shall be maintained constant as an energy saving concept</li> </ul> </li> </ul>
9.	CEIG Approval	<ul style="list-style-type: none"> <li>i. MSI shall be responsible for preparation of electrical schematic layout &amp; physical layout drawings approval for the all electrical installation, equipment, like UPS, inverter, PAC, DG, etc., and obtaining safety certificate from the CEIG. The submission of drawings follow up actions &amp; statutory fee and coordination with CEIG are the also responsibility of the MSI</li> </ul>

#### 6.7.9 Non IT – Diesel Generator: Guidelines and Specifications

S. No.	Nature of Requirement	Guidelines / Specifications
1.		<ul style="list-style-type: none"> <li>i. MSI has to Commission a DG sets comprising of 2 Nos. 630 KVA, for the DC as per following requirements &amp; specifications as per the detailed Technical Specifications</li> <li>ii. Two DG Sets of 630 KVA prime output capacity is required for this project. The set shall automatically start one after the other upon mains power failure depending on the line loads, run up to full speed within 6 seconds of power failure. The set shall be provided with a multiple start mechanism with indication of alarm for "failed to start" condition. A Tachometer switch shall provide control for the start mechanism and also for the "run" indications. The set shall be skid mounted on independent foundation. The acoustic treatment shall ensure a maximum sound pressure not more than 68 dB (A) at 1 meter from the room during the day and 45 dB (A) at the neighbour's premises during night, while running on partial or full load. This condition shall apply to the engine exhaust noise levels also. A vertical type</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		"Critical" silencer shall be fitted on the exhaust pipe after the flexible coupling to reduce the exhaust noise. The exhaust gases shall be piped to the top of the building covering full height of the building. The pipe shall be thermally insulated with ceramic insulation and covered overall with aluminium jacketing. The exhaust pipe and Critical Silencer shall be fixed on a steel structure which shall be rigidly fixed to external wall vertically.
2.	Engine	i. The basic diesel engine shall be Water cooled diesel engine with exhaust Turbo charging and charge air cooling, four valve, individual cylinder heads with exhaust valve rotators, fuel oil pump, fuel duplex filter with diverter valve, fuel injection system, electronically controlled injection, lube oil circulation and coolant thermostats for main cooling and charge air cooling circuit, necessary drives, dry exhaust manifolds, vibration dampers, all necessary pipe work, electric starter suitable for 24 V DC, Generator 28V DC, Electronic speed governor, Fuel filters, Oil dip stick, Oil extraction equipment with hand pump, set of air filters including maintenance indicators, exhaust bellows with connecting flange.
3.	Generator	i. Two Nos. 630KVA Output, 415 Volts, 3 Phase, 50 Hz Generator with Class F Insulation for both stator and rotor with high response static exciter and automatically operated regulator suitable to maintain the voltage within 1% of set value having response time not more than 1 second.
4.	Switch Board - Auto Sync Panel	i. The Switch Board shall be of standard design, free standing, and dust and vermin proof and wired up to terminals ready for installation. The Switch board with Auto Synchronizing Facility included Auto Start and Auto OFF facility
5.	Auto start logic	i. The DG set with enclosure and Auto Start Logic. The Panel should have provision to receive reference EB Supply through potential free contacts to enable connection of external audio alarm in case EB Supply has resumed. Separate battery charger cost to be indicated and the reference EB Supply can be used to charge the batteries. The Auto Start Logic shall be in such a way that the moment EB supply has failed or if the voltages reduce to a pre-determined level, it shall be detected through a voltage monitor and a command shall be given to DG to start with a timer. After the DG voltage has built up to a certain level, the command for changing over of motorized MCCBs from EB to DG or vice versa shall be given. When the EB supply gives normal voltage or has resumed, the command to change over shall be issued

S. No.	Nature of Requirement	Guidelines / Specifications
		with a timer. However, the stopping of the DG shall be only after the DG has run for about 5 minutes on no load basis for it to cool down
6.	Battery chargers and battery	<ul style="list-style-type: none"> <li>i. 24 Volts Battery with Float cum boost charger</li> <li>ii. Proper DC Charging circuits shall be incorporated in the control panel to boost and trickle charge the 24 V DC batteries used for starting the engine. The Control circuit voltage shall be 48 V DC. Proper DC charging circuits shall be incorporated in the Control Panel to boost and trickle charge the 48 V batteries used to power the control circuit. The selection of battery shall be done in such a way that the batteries shall be able to power the circuit even if charging does not take place for 48 hours</li> </ul>
7.	Cables	<ul style="list-style-type: none"> <li>i. Power cables &amp; Control cables are interconnected to use between Generator and Auto Sync Auto load Sharing panel. The required cables for all auxiliary equipment are to be included in the scope of supply</li> <li>ii. All Starters and auxiliary devices / drives if any required should be included in the scope of supply Audio Alarm and Indicators. A separate 24 Window annunciation panel shall be installed in the panel for indicating the following conditions on both sets. A common alarm shall also be sound locally <ul style="list-style-type: none"> <li>a. Engine Run Condition</li> <li>b. Set failed to start</li> <li>c. High Water temperature</li> <li>d. Low Lube Oil Pressure</li> <li>e. Engine Over Speed</li> <li>f. System Power ON</li> <li>g. MCCB Open</li> <li>h. Under Voltage</li> <li>i. Over Voltage</li> <li>j. Frequency Out of Limit</li> <li>k. Over current trip</li> <li>l. Earth Fault</li> <li>m. Reverse Power Trip</li> <li>n. Reverse KVA Trip</li> <li>o. Low and High Fuel level</li> <li>p. Fail to Synchronize</li> <li>q. Load exceeding limit</li> <li>r. Low and High Coolant level in the radiator</li> <li>s. High Alternator Stator temperature</li> <li>t. High Alternator Bearing temperature Alarm</li> <li>u. Restricted earth fault trip.</li> </ul> </li> </ul>
8.	Audio Alarm	<ul style="list-style-type: none"> <li>i. Audio Alarm along with indication shall be provided whenever the synchronizing batteries as well</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<ul style="list-style-type: none"> <li>ii. As the control circuit batteries reach a voltage level below 20 V and 40 V respectively</li> </ul>
9.	Auto Manual Selector Switch	<ul style="list-style-type: none"> <li>i. The function of the Auto Manual Selector switch is to make the operation of the entire panel including operation of change over MCCBs. D G Set starting, stopping etc., selectable between Auto &amp; Manual.</li> <li>ii. Care should be taken in such a way that the panel does not remain partly in Auto and partly in Manual mode when the switch is operated.</li> </ul>
10.	Measuring Devices in Control Panel	<ul style="list-style-type: none"> <li>i. The following Meters shall be provided in the Control Panel Compartment:-</li> <li>ii. DC Ammeter in the DG Charging Kit</li> <li>iii. DC Voltmeter to measure battery voltage</li> <li>iv. DC Ammeter in the trickle charging Kit.</li> <li>v. DG Set speed in RPM</li> <li>vi. Hours Run Meter</li> <li>vii. 2 Nos. CTs of 1000/ 5 A of Class 5 P 10 for Protection.</li> </ul>
11.	Duty Conditions	<ul style="list-style-type: none"> <li>i. The Generator shall be capable of starting and running continuously for about 12 hours</li> </ul>
12.	General	<ul style="list-style-type: none"> <li>i. The DG must be stiffened properly and reading for noise and vibration at full variable condition to be checked before dispatch to Site. Expansion bellow</li> <li>ii. s to be provided before and after silencer</li> <li>iii. MSI would be responsible for conducting the Load Test of D.G set for 6 hours with Diesel (Load to be arranged by the Tenderer)</li> <li>iv. All consumables towards testing of DG at the factory and project site shall arranged by the MSI till the issue of commissioning certificate</li> <li>v. MSI shall obtain permission / approval from the Board for the installation of the DG Set as per exact Rules at their own cost</li> <li>vi. BMS integration through MODBUS protocol with RS485 interface should be provided</li> </ul>

#### 6.7.10 Non IT - UPS: Guidelines and Specifications

S. No.	Nature of Requirement	Guidelines / Specifications
1.		<ul style="list-style-type: none"> <li>i. MSI has to Commission a UPS system comprising of 2Nos. 250 KVA, 2 Nos. 20 KVA UPS with 30minutes SMF battery backup for the ICCC and DC as per requirements &amp; specifications as per the detailed Technical Specifications as given in the tender. The civil works like excavation, construction and installation of foundation, trenches; Hume pipes etc. shall be in the</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		scope of the MSI. The power cabling as specified in the BOQ shall be in the scope of the contractor. The complete signal cabling as required in the UPS room between various equipment shall be in the scope of the contractor. The UPS shall communicate to the BMS through a RS485 port-MODBUS/BACNET protocol. All parameters of the UPS including alarms as displayed on the UPS shall also be displayed real time on the PC screen.
2.	Configuration	<ul style="list-style-type: none"> <li>i. 2 Nos of 250 KVA UPS connected in Dual bus (LBS) configuration for Servers in independent panel</li> <li>ii. 2 x 20 KVA UPS connected in PRS for miscellaneous loads.</li> </ul> <p>Note: All UPS should have Inbuilt Isolation transformer</p>
3.	System Specifications	<ul style="list-style-type: none"> <li>i. The design, manufacturing, testing, installation and performance of equipment and components there have included in this specification, shall comply with all currently applicable Indian &amp; IEC Standards. This specification covers the requirements for design, manufacture, supply, installation and commissioning of UPS &amp; Batteries as specified in the design data and Bill of quantities /schedule of quantities (BOQ)</li> </ul>
4.	UPS specifications	<ul style="list-style-type: none"> <li>i. This specification is for a three phase, on line, continuous operation, solid-state uninterruptible power supply (UPS). The UPS has to operate in conjunction with the existing building electrical system backup power protection, and power distribution for the critical loads. The UPS shall be True Online with delta or double conversion technology. The power flow is through Rectifier and then the Inverter. The rectifier shall be with SCR (12 Pulse) as power conversion element. The inverter shall be with IGBT design and with state of the art sine wave control technology, for the 350 KVA UPS which shall ensure high quality of power conditioning. The design must provide for a mean time between failures, field proven minimum of 120,000 hours. For ease of maintenance and service, the UPS must have field replaceable modular sub-assemblies. All material comprising the UPS module must be new, of current manufacture and should not have been in prior service except as required during factory testing. The UPS module must contain no PVC materials.</li> <li>ii. The UPS shall be capable to operate and charge battery even when the incoming supply goes to +/-15% over the nominal (300V to 480V). It shall be ensured that the battery charging should be possible at minimum input</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>supply voltage condition. Battery should not be discharged up to the minimum input supply voltage level. Being a high-end data centre application a Full-fledged and highly reliable Power Conditioning system (UPS) is desirable. The system should have a close voltage regulation viz. 400 +/- 1% for the entire computer / server load spectrum. Also the output frequency correction of +/- 1% is preferable when the input frequency goes out of tolerance and system should not go to battery mode during 47Hz input or 53 Hz input. This might happen with DG sets some time.</p> <p>iii. The system shall have the highest industry efficiency, employing appropriate conversion technology and built in isolation transformer for load safety and cost effective operation all through.</p> <p>iv. Since power quality is a key factor for load safety and mains safety (both output and input of the UPS) the following major specs may be called for. Voltage Regulation and Transient Response: Voltage regulation should be 1% of the set value, and transient response should be less than 5% with fastest correction (&lt; 5 milliseconds).</p> <p>Note: The output quality is a major concern and therefore very low Total Voltage harmonic Distortion is required to be maintained, at all load points especially at Server Input terminals to minimize load side false trips etc. The total number of series power devices may be reduced to ensure high uptime (MTBF) and overall reliability.</p>
5.	Rectifier	<p>i. The rectifier design shall be state of the art PWM rectifier, employing IGBT/SCR as rectifying element along with filters (in case SCR technology) to achieve Input Power Factor is expected to be better than 0.92 and the current harmonic distortion level less than 5%. The Total Voltage harmonic Distortion should be &lt; 5% for 100% non-linear / SMPS /Computer loads. This shall reduce the load side current harmonics to a great extent and the UPS system shall be low impedance type using appropriate technology. The generator rating required for the UPS shall be max.50% more than the rating of input power for the UPS.</p> <p>ii. Float charge: Under nominal operating conditions, the battery charger has to provide a nominal DC bus voltage.</p> <p>iii. Boost charge: The battery charger has to provide a boost charge of 2.27 to 2.40 volts per cell</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>(programmable) for a period of 1 to 24 hours programmable.</p> <p>iv. Battery charger temperature compensation: For protection of the batteries, the unit must monitor the temperature of the batteries. To extend battery life, charge voltage must be compensated for changes in battery temperature.</p> <p>v. Battery charge current limit: The battery charge current limit must be limited to 10% of nominal DC discharge current (programmable to lower level).</p>
6.	Inverter	<p>i. The UPS shall provide state of the art power conditioning. The output waveform shall be pure sine wave with distortion level of less than 2% on 100% linear load and less than 5% on non-linear load. It should support loads with crest factor of 3:1 or higher. The dynamic regulation shall be superior and the UPS should have capability to clear branch circuit fuses (HRC type) – with minimum of 20% rating. The control shall be fully digital employing dual microprocessor or superior technology. The inverter has to be capable of supplying overload current of min. 150% of the system rating for 30 seconds.</p>
7.	Battery	<p>i. The batteries shall be sealed maintenance free lead acid type, the batteries shall be housed in a powder coated open rack complete with battery, inter cell connectors etc. The cabinet shall be cubicle type, floor mounted and powder coated. All sides of the cabinet shall be open and with louvers for ventilation. The battery cabinet shall be designed to allow for ease of maintenance / easy access. Battery type: Sealed valve-regulated, flooded, battery cells designed for high rate of discharge.</p> <p>ii. Design Lifetime: ≥ 5 years</p> <p>iii. DC ripple: Max. 2%</p> <p>iv. Low battery voltage protection: To prevent total discharge or damage to the battery, the UPS must transfer to standby operation when the battery voltage reaches a set minimum voltage level (programmable). If the AC input source has not returned within 10 minutes after "low battery" shutdown, the UPS shall automatically disconnect DC power from the battery to avoid deep discharge.</p> <p>v. A battery-monitoring unit must be part of the system and it shall be capable of monitoring and defining battery capacity. It must be possible to program the unit to perform an automatic battery test every 90 days to test the condition of the battery.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>vi. Battery manufacturing controls: Each battery cell must be clearly identified as to cell type, voltage, and capacity. All cells in the battery have to be tested to verify 100% system capacity. The equipment must be designed and manufactured under a quality assurance program that is controlled and documented by written policies, procedures, or instruction.</p>
8.	Ups Display and Controls	<p>i. Display unit: A microprocessor-controlled display unit shall be located at the front of the UPS cabinet. The display shall consist of an Alpha-numeric backlit LCD display, an alarm LED, and a touch key pad. The UPS should have a minimum of 200 record histories. UPS status messages The display unit shall show the following UPS status messages:</p> <p>ii. Normal operation, load power xxx%</p> <p>iii. Battery operation, time xxx minutes</p> <p>iv. Standby The display unit shall show the following metered parameters:</p> <p>v. Input AC voltage (line-to-line, three-phase simultaneous).</p> <p>vi. Input AC current (line-to-neutral, three-phase simultaneous).</p> <p>vii. Output AC voltage (line-to-line, three-phase simultaneous).</p> <p>viii. Output AC current (line-to neutral, three-phase simultaneous)</p> <p>ix. Battery voltage</p> <p>x. Battery current (charge/discharge)</p> <p>xi. Battery temperature.</p> <p>xii. Output peak current</p> <p>xiii. Input / Output Power - KVA / KW</p> <p>xiv. Input / Output Power Factor</p> <p>xv. Input / Output Frequency</p> <p>xvi. The display unit shall record a log of all active alarms. More than 40 alarm conditions must be monitored. The record shall be in the form of a time and date stamped log of the 500 most recent UPS status and alarm events. These alarm events must be able to be seen thru the RS485 C interface in a designated PC/BMS.</p>
9.	Controls	<p>The following control and operational commands shall be shown on the display unit:</p> <p>i. Silence an audible alarm.</p> <p>ii. Set the alphanumeric display language to English or the alternative language.</p> <p>iii. Display or program the time and date</p> <p>iv. Enable or disable the automatic restart feature.</p> <p>v. Transfer to or from forced battery operation.</p> <p>vi. Program the unit for economy operation.</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<ul style="list-style-type: none"> <li>vii. Program the battery charger.</li> <li>viii. Calculate battery back-up time.</li> <li>ix. Test battery condition on demand.</li> <li>x. Program the unit to periodically test battery condition.</li> <li>xi. Program voltage and frequency windows</li> <li>xii. Calibrate metered parameters</li> <li>xiii. Enable or disable adaptive slew rate. Set maximum slew rate.</li> <li>xiv. Adjust set points for different alarms.</li> <li>xv. Program the remote shutdown contact (enable/disable remote shutdown, polarity, delay.)</li> <li>xvi. Set the delay for the common fault contact.</li> <li>xvii. Program the unit for soft start for use with a generator.</li> </ul>
10.		<p>The following control and operational commands shall be shown on the display unit:</p> <ul style="list-style-type: none"> <li>i. Silence an audible alarm.</li> <li>ii. Set the alphanumeric display language to English or the alternative language.</li> <li>iii. Display or program the time and date</li> <li>iv. Enable or disable the automatic restart feature.</li> <li>v. Transfer to or from forced battery operation.</li> <li>vi. Program the unit for economy operation.</li> <li>vii. Program the battery charger.</li> <li>viii. Calculate battery back-up time.</li> <li>ix. Test battery condition on demand.</li> <li>x. Program the unit to periodically test battery condition.</li> <li>xi. Program voltage and frequency windows</li> <li>xii. Calibrate metered parameters</li> <li>xiii. Enable or disable adaptive slew rate. Set maximum slew rate.</li> <li>xiv. Adjust set points for different alarms.</li> <li>xv. Program the remote shutdown contact (enable/disable remote shutdown, polarity, delay.)</li> <li>xvi. Set the delay for the common fault contact.</li> <li>xvii. Program the unit for soft start for use with a generator.</li> </ul>
11.	UPS ON and OFF Push buttons	<ul style="list-style-type: none"> <li>i. Momentary UPS on and off push button must be provided in a locked user accessible compartment. Upon activation of the on push button, the UPS must automatically connect the UPS output to the load. Upon activation of the off push button, the UPS must remove power from the load</li> </ul>
12.	UPS Potential free contact	<ul style="list-style-type: none"> <li>i. The UPS must be equipped with potential free contacts for indicating:</li> <li>ii. Common fault alarm</li> <li>iii. Battery operation.</li> <li>iv. Other optional indications / control.</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
13.	UPS Communication interface board	<p>i. The system shall have a communication interface board, which shall provide the following communication ports, and it must be possible to use two or more ports simultaneously.</p> <p>1. RS485 serial port</p> <p>2. COM PORT with the following normally open or normally closed potential free contacts:</p> <ul style="list-style-type: none"> <li>a. UPS on.</li> <li>b. Battery operation.</li> <li>c. Battery low.</li> </ul> <p>ii. The UPS shall have to communicate with the BMS on RS485/MODBUS protocol. All hardware / software (with passwords) required for the communication is deemed as included and shall be provided whether expressly mentioned or not.</p>
14.	Remote Display	<p>i. All electrical parameters, faults, alarms etc. must be displayed on a remote alphanumeric LCD display. All alarms shall be displayed with a built in sounder and should be possible to be acknowledged and reset at this remote panel also.</p>
15.	Mechanical Design	<p>i. The UPS, Battery cubicle and Switching cubicle must be housed in a powder coated open rack. All service access must be from the front and top. The cable entry shall be from the Top. The UPS and switching cubicle can be cooled by forced air. The battery cubicle can be cooled by free air ventilation and convection.</p> <p>ii. Performance: The UPS system shall be designed for full power rating. The MSI needs to specify output current at rated power factor and considering 45 Deg. as ambient temperature.</p> <p>iii. Efficiency: The overall efficiency of systems shall be very high and minimum as specified.</p> <p>iv. Accessories: Only MCCB shall be provided in battery path. Switch fuse unit for battery isolation is not acceptable. The monitoring software and BMS compatibility using RS485 MODBUS/BACENT protocol and the UPS to battery cables shall be integral part of Systems and made available at no extra cost.</p> <p>v. Total Power Protection: The multiple power protections to the rectifier as well as inverter and to the load shall form integral part of UPS design.</p> <p>vi. Codes of Operation: The UPS has to operate as an online system in the modes listed below: Normal: The rectifier / inverter charger has to operate in an online mode to continuously regulate the power to the load. The inverter / battery charger also has to</p>

S. No.	Nature of Requirement	Guidelines / Specifications
		<p>derive power from the AC input source and supply DC power to float charge the battery.</p> <p>Mains A.C Input power failure: Upon failure of the AC input source, all the output loads must continue to be supplied by the inverter without any break by switching over to battery derived input power. There must be no break / interruption of power to the load upon failure or restoration of the AC input source.</p> <p>Recharge: Upon restoration of the AC input source, the battery charger must simultaneously recharge the battery and regulate the power to the critical load.</p> <p>vii. STANDARDS: The UPS and all its components, SMF battery etc. shall comply with all the relevant ISI and global standards and norms.</p>
16.	Miscellaneous	<ul style="list-style-type: none"> <li>i. The contactors should comply with the latest BSEN 60947 - 4 -1 / IEC 60947 - 4 All contactors must be rated for AC3 duty.</li> <li>ii. The contactors should be capable of frequent switching and should operate without derating at 600 deg C for AC3 applications. They should be climate proof as standard .The coil of the contactor should have class H insulation to support frequent switching.</li> <li>iii. The contactor should be modular in design with minimum inventory requirements and built in mechanically interlocked 1NO 1NC auxiliary contact up to 32A.</li> <li>iv. Wherever D.C control is required, the contactor should have wide range (0.7 to 1.25Uc) D.C coil with built in interference suppression as standard. The control and power terminals should be at separate layers preferably with colour coding (black for power and white for control).</li> </ul>
17.	Control and Selector Switches	<ul style="list-style-type: none"> <li>i. Control and selector switches shall be of the rotary type, having enclosed contacts, which are accessible by removal of the cover. Control and selector switches for instruments shall be flush mounted on the front of the panels and desks. Local / Remove selector switches when located on switchgear cubicles, shall be mounted inside the relay compartment at an accessible location.</li> <li>ii. All control switches shall be of the spring return to normal type. Circuit breaker control switches on switchgear cubicles shall be lockable in the trip position. Control switches shall have momentary contacts. Circuit breaker control switches shall be provided with a sequencing device to prevent repetitive closing operations without first moving to the trip position. Selector switches shall be of the stay - put maintained contact type.</li> </ul>

S. No.	Nature of Requirement	Guidelines / Specifications
		iii. Control switches shall be provided with pistol grip handles. Selector switches shall be provided with round, knurled handles. All handles shall be black in colour. Properly designated numbering plates clearly marked to show the operating positions shall be provided with all switches.
18.	Standards for commissioning of UPS	i. The electrical installation work covered by this specification shall unless otherwise stated comply with the requirements of the latest edition of relevant Indian Standard, statutory regulations and codes of practices
19.	Standards	i. Indian Electricity Rules. -1956 ii. Tariff advisory committee. - Approvals. iii. BSEN 60947 / IEC 60947: Code of practice for selection, installation & maintenance of Switch gear and control gear iv. BS 3535: Isolation Transformers BS CODE of practice for earthling v. BS 6651 – 1985 Code of practice for protection of building and allied structures against lightning. vi. BS CODE of practice for electrical wiring installation.

## 6.8 Communication Network

- I. There shall be redundant network connectivity at Junction Box level. Typically junction boxes shall be part of ring network as per MSI solution.
- II. The network connectivity provided at Junction boxes shall be scalable to carry bandwidth up to 1Gbps.
- III. City WAN network shall be aggregated into ISP links that shall be connected at Core router in high-availability mode and MSI should include required number & type of Ports in the core router to terminate the WAN ISP links with some spare ports for future use.
- IV. The core & Internet router interfaces shall be sized as per the termination links provided by ISP and shall meet all functional and technical requirements as mentioned in this RFP.
- V. Network is taken on lease as a service, therefore all kinds of maintenance work or upgrades on the network shall be taken care by MSI at his own expense without any charge to ASCL.
- VI. The design and construction of network cabling used shall be inherently rugged and robust under all conditions of installation, operations, storage and transport.
- VII. The cable shall be able to work in all field level environmental conditions and should be protected against corrosion or damage from rodents and other pests.

## 7. Technical Specifications Hardware

### 7.1 City Surveillance

#### 7.1.1 Standard GI Pole

S. No.	Nature of requirement	Minimum Requirement Specifications
POLE-TR-01	General Requirement	Shall be minimum 20ft (6.5mts) height as per NHAI norms
POLE-TR-02	General Requirement	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate size 30x30x15 cms suitable for wind speed 50m/sec with suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980)
POLE-TR-03	Foundation	The pole would be fixed on an adequate and strong foundation so as to withstand city weather conditions and wind speed of 150km / hr
POLE-TR-04	Foundation	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100cms or better
POLE-TR-05	Protection	Lighting arrestors with proper grounding
POLE-TR-06	Sign Board with number plate	Sign board depicting the area under surveillance and with the serial number of the pole
POLE-TR-07	Height	The height of the pole shall be as per requirement of the location varying from 6.Mts to 12/15 Mts.

#### 7.1.2 Cantilever GI Pole

S. No.	Nature of requirement	Minimum Requirement Specifications
POLEA-TR-01	General Requirement	Shall be minimum 6.00mts height as per NHAI norms Wall Thickness: 4.5 mm Overhang: 9mtr or 6 or 3 mtr. depending on lanes
POLEA-TR-02	Quality	Mild Steel (M.S) Tubular Pipe ( B-Class) as per IS-1239 (Part-1)-193
POLEA-TR-03	Base Plate	Size 400 mm x 400 mm x 16 mm thick welded to the bottom of the signal pole
POLEA-TR-04	Foundation	Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality

S. No.	Nature of requirement	Minimum Requirement Specifications
		<p>should not be impacted due to wind in different climatic conditions) Expected foundation depth of minimum 100cms or better</p> <ul style="list-style-type: none"> <li>• Length: 600 mm</li> <li>• Width: 600 mm</li> <li>• Depth: 150 mm</li> <li>• Bolts: 25 mm/8 Nos.</li> <li>• 8 mm Rings: 8 Nos.</li> <li>• 16 mm Rods: 12 Nos.</li> </ul>
POLEA-TR-05	Protection	Lighting arrestors with proper grounding
POLEA-TR-06	Sign Board with number plate	Sign board depicting the area under surveillance and with the serial number of the pole
POLEA-TR-07	Paint	Pole painted with two coats of primer and in addition bituminous painting for other bottom 1.5 M portion of pole
POLEA-TR-08	Arms	The pole shall be able to support 2 arms of 6 meter length each on either side and suitable for ANPR and Surveillance camera mounting

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

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

S. No.	Nature of requirement	Minimum Requirement Specifications
FBCFR-TR-01	Image Sensor	1/2.8" progressive scan RGB CMOS
FBCFR-TR-02	Operating Frequency	50 Hz
FBCFR-TR-03	Day/ Night Operation	Yes with IR Cut Filter
FBCFR-TR-04	Minimum Illumination	Colour: 0.2 Lux @ 30 IRE B/W: 0.01 @ 30 IRE 0 Lux with Built in or External IR, IR Range 50 Meters
FBCFR-TR-05	Low light Capability	The camera shall be able to provide usable Colour video in low light conditions
FBCFR-TR-06	Lens	5-50mm IR corrected, CS-mount lens, P-Iris
FBCFR-TR-07	Electronic Shutter	1/30 to 1/10000 s or better
FBCFR-TR-08	Image Resolution	1920 x 1080, 1280 x 720, 800 x 450, 480 x 270, 320 x 240
FBCFR-TR-09	Compression	H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG
FBCFR-TR-10	Frame Rate and Bit Rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate

S. No.	Nature of requirement	Minimum Requirement Specifications
FBCFR-TR-11	Video Streams	The camera shall be able to setup and stream out minimum three (3) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently up to Full HD @ 30 FPS
FBCFR-TR-12	Motion Detection	Yes built in with multiple configurable areas in the video stream
FBCFR-TR-13	Pan Tilt Zoom	Digital PTZ
FBCFR-TR-14	Electronic Exposure & Control	Automatic/ Manual
FBCFR-TR-15	Wide Dynamic Range	120 dB or better
FBCFR-TR-16	Backlight Compensation	Required
FBCFR-TR-17	Privacy Masks	Minimum 20 configurable 3D zones
FBCFR-TR-18	Connectors	1 Input & 1 Output for Alarm Interface
FBCFR-TR-19	Audio	Two way Audio
FBCFR-TR-20	Event Triggers	Intelligent video, Edge Storage event, External Input, Audio Level, Motion Detection, Day/Night Mode, Network, Time scheduled, 3rd Party Analytics, Manual Trigger, Alarm Input Trigger
FBCFR-TR-21	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and TCP, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, External Output activation
FBCFR-TR-22	Edge Storage	SD Card Slot with minimum 64GB Support Class 10 speed
FBCFR-TR-23	Remote Focus	Ability to fine tune focus of camera remotely
FBCFR-TR-24	Storage	The Cameras shall have the feature to directly record the videos/ images onto NAS/SAN without any Software or integration
FBCFR-TR-25	Protocols	IPv4/v6, HTTP , HTTPS b, SSL/TLS b,QoS Layer 3 DiffServ, FTP , CIFS/SMB, SMTP, Bonjour, UPnP™,SNMPv1/v2c/v3 (MIB - II), DNS,DynDNS, NTP, RTSP, RTP,TCP, UDP,IGMP,RTCP,ICMP,DHCP,ARP,SOCKS
FBCFR-TR-26	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.
FBCFR-TR-27	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
FBCFR-TR-28	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost

S. No.	Nature of requirement	Minimum Requirement Specifications
FBCFR-TR-29	Logs	The camera shall provide minimum logs of latest connections, access attempts, users connected, changes in the cameras etc.
FBCFR-TR-30	Interface	RJ 45, 100 Base TX
FBCFR-TR-31	Enclosure	IP66 casing made of Polycarbonate/Aluminium, IK 10
FBCFR-TR-32	Power requirements	PE IEEE 802.3af / POE+ IEEE 902.3at compliant
FBCFR-TR-33	Operating Temperature	-10 °C to 50 °C
FBCFR-TR-34	Operating Humidity	Humidity 20-95% RH (condensing)
FBCFR-TR-35	Certification	UL, CE, FCC, IEC
FBCFR-TR-36	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain free of cost
FBCFR-TR-37	Housing, Mount and IR	Shall be of the same make of OEM or better
FBCFR-TR-38	Onvif S	Required
FBCFR-TR-39	Warranty	Min 5 Years OEM Warranty
FBCFR-TR-40	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
FBCFR-TR-41	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
FBCFR-TR-42	White Balance	Auto and Manual setting
FBCFR-TR-43	Support	The system should not be an end of life / end of service product
PTZ-TR-44	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.
PTZ-TR-02	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols

Cameras shall meet all the above requirements and key requirements mentioned in function requirement specification

#### 7.1.4 Bullet Indoor Camera - Face recognition

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

S. No.	Nature of requirement	Minimum Requirement Specifications
BCS- TR -01	Image Sensor	1/3" progressive scan RGB CMOS or better
BCS- TR -02	Operating Frequency	50 Hz
BCS- TR -03	Day/ Night Operation	Yes with IR Cut Filter
BCS- TR -04	Minimum Illumination	Colour: 0.3 Lux @ 30 IRE F1.4; 0 Lux with IR
BCS- TR -05	Mechanical Pan Tilt Adjustment	Pan: ± 135°, Tilt: 0°- 90°

S. No.	Nature of requirement	Minimum Requirement Specifications
BCS- TR -06	Lens	3 - 10 mm, IR corrected, P-Iris, Megapixel Lens with remote zoom and focus
BCS- TR -07	Electronic Shutter	1/30 s to 1/10000 s or better
BCS- TR -08	Image Resolution	1920 x 1080 or better
BCS- TR -09	Compression	H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG
BCS- TR -10	Frame Rate and Bit Rate	Up to 50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate. In CBR Priority to be defined for Video quality or frame rate and the bandwidth upper limit shall not exceed the defined limit
BCS- TR -11	Image reproduction	The camera shall have the capability to produce Coloured video images in low light conditions
BCS- TR -12	Video Streams	The camera shall be able to setup and stream out minimum three (3) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently
BCS- TR -13	Motion Detection	Yes built in with multiple configurable areas in the video stream
BCS- TR -14	Image Configuration	The Camera shall be able to Include or Exclude any area of any size/ dimension within the scene in order to Eliminate False alarm and also optimize the bandwidth and storage
BCS- TR -15	Pan Tilt Zoom	Digital PTZ
BCS- TR -16	Wide Dynamic Range	120 dB or better
BCS- TR -17	Backlight Compensation	Required
BCS- TR -18	IR	30 Meter (Built in or External) Optimized IR with adjustable intensity and angle
BCS- TR -19	Alarm Connectors	1 Input & 1 Output for Alarm Interface
BCS- TR -20	Event Triggers	Live Stream Accessed, Motion Detection, Day/Night Mode, Network, Temperature, , Camera Tampering, Edge Storage Disruption, Video Analytics, Manual Trigger,
BCS- TR -21	Event Actions	FTP, HTTP, network share, email Notification: email, PTZ function, Edge Storage/ NAS Storage, Pre & Post Alarm Recording, Actions configurable by web interface, WDR Mode, External Output Trigger, Text Overlay
BCS- TR -22	Edge Storage	SD Card Slot with 64GB Support Class 10 speed
BCS- TR -23	Protocols	IPv4/v6, HTTP , HTTPS, SSL/TLS, QoS Layer 3 DiffServ, FTP , CIFS/SMB, SMTP, Bonjour, UPnP,SNMPv1/v2c/v3 (MIB - II), DNS, DynDNS, NTP, RTSP, RTP,TCP, UDP, IGMP,RTCP,ICMP,DHCP,ARP,SOCKS, SSH

S. No.	Nature of requirement	Minimum Requirement Specifications
BCS- TR -24	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc.
BCS- TR -25	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log
BCS- TR -26	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
BCS- TR -27	Interface	RJ 45, 100 Base TX
BCS- TR -28	Memory	512 MB RAM, 256 MB Flash or better
BCS- TR -29	Enclosure	IP66 rated and NEMA-4X-rated casing Polycarbonate/Aluminium, IK 08
BCS- TR -30	Power requirements	PE IEEE 802.3af / POE+ IEEE 902.3at compliant
BCS- TR -31	Operating Temperature	-10 °C to 60 °C
BCS- TR -32	Operating Humidity	Humidity 20–90% RH (condensing)
BCS- TR -33	Certification	UL, CE, FCC, IEC,
BCS- TR -34	Application Programmers Interface	The interface shall be available for integration with 3rd party analytics and applications in public domain
BCS- TR -35	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
BCS- TR -36	Mount	Wall Mount/ Pole Mount
BCS- TR -37	Onvif S	Required
BCS- TR -38	Warranty	5 Years OEM warranty
BCS- TR -39	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
BCS- TR -40	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
BCS- TR -41	White Balance	Auto and Manual setting
BCS- TR -42	Support	The system should not be an end of life / end of service product
PTZ-TR-43	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.
PTZ-TR-44	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols

Cameras shall meet all the above requirements and key requirements mentioned in Functional Requirement Section

### 7.1.5 360 Degree Panoramic Camera

S. No.	Nature of requirement	Minimum Requirement Specifications
PCT-FR-01	Image Sensor	4 x 1/2.8" progressive scan CMOS or better
PCT-FR-02	Operating Frequency	50 Hz
PCT-FR-03	Day/ Night Operation	Yes with Built-in Automatic IR Cut Filter
PCT-FR-04	Minimum Illumination	Colour: 0.3 Lux @ 30 IRE
PCT-FR-05	Lens	Varifocal, 3-6 mm, F1.8-2.6, remote focus, remote zoom
PCT-FR-06	Field of View	96°-56° each sensor
PCT-FR-07	Electronic Shutter	1/32500 s to 1/25
PCT-FR-08	Image Resolution	4 x 1920x1080 (1080p)
PCT-FR-09	Compression	"H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG"
PCT-FR-10	Frame Rate and Bit Rate	Up to 25/30 fps
PCT-FR-11	Video Streams	The camera shall be able to setup and stream out minimum eight (8) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently up to Full HD @ 30 FPS
PCT-FR-12	Motion Detection	Yes built in with multiple configurable areas in the video stream
PCT-FR-13	Image settings	Saturation, contrast, brightness, sharpness, WDR, white balance, exposure control, exposure zone, fine tuning of behaviour at low light, defogging, rotation: 0°, 90°, 180°, 270° including Corridor Format, text and image overlay, privacy mask, compression
PCT-FR-14	Intelligent capabilities	Live Stream Accessed, Motion Detection, Network, Active Tampering, Edge Storage Disruption, 3rd Party Analytics, Manual Trigger, Virtual Input, Built in pixel counter
PCT-FR-15	Event Actions	File upload: FTP, HTTP, network share and email Notification: email, HTTP and Overlay text, pre- and post-alarm video buffering, SNMP trap
PCT-FR-16	Edge Storage	Built in SD card slot with support up to 64 GB with Class 10 speed
PCT-FR-17	Storage	Support for recording to dedicated network-attached storage
PCT-FR-18	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera
PCT-FR-19	Protocols	IPv4/v6, HTTP, HTTPS b, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP™, SNMPv1/v2c/v3 (MIB - II), DNS, DynDNS,

S. No.	Nature of requirement	Minimum Requirement Specifications
		NTP, RTSP, RTP, TCP, UDP, IGMP, RTCP, ICMP, DHCP, ARP, SOCKS
PCT-FR-20	Text Overlay	Date & time, and a customer-specific text, camera name, graphical image etc
PCT-FR-21	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log, Centralized Certificate Management
PCT-FR-22	Firmware Upgrade	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
PCT-FR-23	Logs	The camera shall provide logs of latest connections, access attempts, users connected, changes in the cameras etc.
PCT-FR-24	Interface	RJ 45, 100 Base TX
PCT-FR-25	IR illumination	External IR illumination up to distance of 100 meters from camera
PCT-FR-26	Enclosure	IP66, IK09 impact-resistant aluminium or plastic casing with polycarbonate hard-coated dome,
PCT-FR-27	Memory	1GB RAM, 256 MB Flash or better
PCT-FR-28	Power requirements	Power over Ethernet (PoE) IEEE 802.3af/802.3at
PCT-FR-29	Operating Temperature	-10 °C to 65 °C
PCT-FR-30	Warranty	10-95% RH (condensing)
PCT-FR-31	Certification	UL, CE, FCC, IEC, EN
PCT-FR-32	Application Programmers Interface	The camera shall be fully supported by an open and published web service using REST API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications
PCT-FR-33	Mount	Wall/ Ceiling/ Surface/ Pole
PCT-FR-34	Onvif S	Required
PCT-FR-35	Warranty	5 Years OEM Warranty
PCT-FR-36	Security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
PCT-FR-37	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
PCT-FR-38	White Balance	Auto and Manual setting
PCT-FR-39	Support	The system should not be an end of life / end of service product
PTZ-TR-40	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.
PTZ-TR-02	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols

### 7.1.6 PTZ Camera

S. No.	Nature of requirement	Minimum Requirement Specifications
PTZ-TR-01	General Requirements	The camera should be manufacturer's official product line designed for 24x7x365 use.
PTZ-TR-02	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols
PTZ-TR-03	Image Sensor with WDR	True WDR 120 db or better, 1/2.8' Progressive CMOS Sensor or better with minimum 2 MP resolution
PTZ-TR-04	Resolution	Camera should be Full HD PTZ 1920 (w) x1080 (h)
PTZ-TR-05	Frame Rate	Min 25 fps
PTZ-TR-06	Lens specs	Auto-focus, 4.4 – 84.6 mm (corresponding to 18x)
PTZ-TR-07	Minimum illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE) or better
PTZ-TR-08	Pre-set Positions	256 or better, Pre-set tour
PTZ-TR-09	PTZ	Pan: 0 to 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 20x optical zoom and 10x digital zoom Auto-Tracking
PTZ-TR-10	General	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently
PTZ-TR-11	Outdoor Protection	The camera should be complete with IP 66 rated housing, Connectors, Camera Mounts, Power Supply and all Ancillary Equipment & all accessories
PTZ-TR-12	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, 802.1X, IPv4/v6, QoS, DNS, DDNS, NTP
PTZ-TR-13	Compression Capability	" H.265 compression or 3 Mbps and lower speed at 1920 X 1080 @ 30 FPS per stream and MJPEG"
PTZ-TR-14	Noise Reduction	Ultra DNR (2D/3D)
PTZ-TR-15	Certificate	CE, UL, FCC, ONVIF
PTZ-TR-16	Industry Standards	ONVIF S Compliant
PTZ-TR-18	Miscellaneous	Power Supply : External 12V /24V/48V DC/ POE+
PTZ-TR-19	Ethernet	Connectors: 10Base-T/100Base-TX
PTZ-TR-20	Miscellaneous	Cable routing through base or rear of housing
PTZ-TR-21	Miscellaneous	Operating conditions unit: -10° C to 50° C or better, humidity 0% to 95% non-condensing

S. No.	Nature of requirement	Minimum Requirement Specifications
PTZ-TR-22	Miscellaneous	Tamper Proof
PTZ-TR-23	Miscellaneous	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
PTZ-TR-24	Support	The system should not be an end of life / end of service product
PTZ-TR-25	Audio	Audio capture Capability
PTZ-TR-26	Local Storage	32GB or higher
PTZ-TR-27	Security	Password Protection, HTTPS encryption, IEEE 802.1X
PTZ-TR-28	S/N Ratio	≥ 50dB
PTZ-TR-29	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
PTZ-TR-30	Mounting Accessories	For pole and surface mount with L/C Brackets
PTZ-TR-31	IR Illumination	Internal > 150 meters

#### 7.1.7 Public Address System with Integrated Audio Amplifier

S. No.	Nature of requirement	Minimum Requirement Specifications
PAS-TR-01		The system should allow streaming in both local network and internet and operable from Central command centre. System should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all location (1: many) simultaneously. The PAS should also support both, Live and pre-recorded inputs
PAS-TR-02	General	Unlimited number of both sources and incomers of stream in the system
		Division of the speakers into independently controlled groups, minimum 2 Speaker, to be used for public address system at a location.
PAS-TR-03		Possibility to setup an independent operating
PAS-TR-04		Audio playback from a file or an external source
PAS-TR-05		Audio streams mixing - playlist creation support
PAS-TR-05	Audio	One-way/two-way (mono)
PAS-TR-06	Compression	G.711 PCM 8 kHz, G.726 ADPCM 8 kHz, WAV, MP3 in mono/stereo from 64 kbps to 320 kbps. Constant and variable bit rate. Sampling rate from 8 kHz up to 48 kHz. Configurable bit rate
PAS-TR-07	input/output	Built-in microphone with frequency 50 Hz - 16 kHz (for testing purpose)
PAS-TR-08	Max sound pressure level	>120 dB

S. No.	Nature of requirement	Minimum Requirement Specifications
PAS-TR-09	Frequency response	280 Hz -12.5 kHz
PAS-TR-10	Coverage	Minimum 70° horizontal by 95° vertical (at 2 kHz)
PAS-TR-11	Built In Amplifier	7 W Class D amplifier
PAS-TR-12	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1X network access control, Digest authentication, User access log
PAS-TR-13	Supported protocols	IPv4/v6, HTTP, HTTPS, SIP, SSL/TLS, QoS Layer 3 DiffServ, FTP, CIFS/SMB, SMTP, Bonjour, UPnP, SNMP v1/v2c/v3 (MIB-II), DNS, DynDNS, NTP, TCP, UDP, IGMP, ICMP, DHCP, ARP, SOCKS, SSH
PAS-TR-14	Audio functionality	The horn speaker shall support SIP for integration with VoIP, peer-to-peer or integrated into SIP/PBX
PAS-TR-15	Language	The horn speaker shall provide a function for altering the language of the user interface, and shall include support for at least English and Hindi
PAS-TR-16	Installation and Maintenance	The horn speaker shall include a test functionality allowing a test tone sequence to be generated and measured by the built-in microphone to verify full functionality
PAS-TR-17	API	Horn speakers shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications
PAS-TR-18	Firmware	The firmware upgrade shall be done through web interface, The firmware shall be available free of cost
PAS-TR-19	Audio Speaker test	Shall be available for testing speaker functionality
PAS-TR-20	Event triggers	Call, Virtual inputs
PAS-TR-21	Event actions	File upload via HTTP/network share/ email Notification via email, HTTP and TCP Play audio clip Send Auto Speaker Test Send SNMP trap Status LED
PAS-TR-22	Built-in installation aids	Test tone
PAS-TR-23	Functional monitoring	Auto Speaker Test, Connection verification, Built-in system logging
PAS-TR-24	Housing	Impact-resistant aluminium, IP66 rated
PAS-TR-25	Built in Memory	Minimum 256 MB RAM, 256 MB Flash

S. No.	Nature of requirement	Minimum Requirement Specifications
PAS-TR-26	Power	Power over Ethernet (PoE) IEEE 802.3af/802.3at Type 1 Class 3 (max 14 W)
PAS-TR-27	Connectors	RJ45 10BASE-T/100BASE-TX PoE
PAS-TR-28	Operating Temperature	0°C to 50 °C
PAS-TR-29	Operating Humidity	Humidity 10-100% RH (condensing)
PAS-TR-30	Certification	EN, CE, FCC, UL, IEC
PAS-TR-31	Warranty	5 Years OEM Warranty

### 7.1.8 CAT 6 Cable

S. No.	Nature of requirement	Minimum Requirement Specifications
CAT-TR-01	Environmental Space	Plenum
CAT-TR-02	Suitable Applications	Networking Horizontal Cable, 1000Base-T (Gigabit Ethernet), 100Base-T (Fast Ethernet), 10Base-T (Ethernet), 100BaseVG, ANYLAN, 155ATM, 622ATM, ANSI.X3.263 FDDI / TP-PMD, NTSC/PAL Component or Composite Video, AES/EBU, Digital Video, RS-422, Noisy Environments, 250 MHz Category 6
CAT-TR-03	AWG Size	23
CAT-TR-04	Material	FEP - Fluorinated Ethylene Propylene
CAT-TR-05	Outer Shield Material	Aluminium Foil-Polyester
CAT-TR-06	Drain wire Material	TC - Tinned Copper
CAT-TR-07	Outer Jacket Material	LS PVC - Low Smoke Polyvinyl Chloride
CAT-TR-08	Cabling	Patented Central X-spline
CAT-TR-09	Conductor DCR	9.38 Ohm/100m
CAT-TR-10	Capacitance	160 pF/100m
CAT-TR-11	Installation Temp Range	0°C To +50°C
CAT-TR-12	UL Temp Rating	75°C
CAT-TR-13	Storage Temp Range Operating Temp Range	-20°C To +75°C -20°C To +75°C
CAT-TR-14	Bulk Cable Weight	44 lbs/1000ft
CAT-TR-15	Max Recommended Pulling	25 lbs

S. No.	Nature of requirement	Minimum Requirement Specifications
	Tension	
CAT-TR-16	Min Bend Radius/Minor Axis	1.0 in
CAT-TR-17	Min Bend Radius / Installation	2.25 in
CAT-TR-18	ANSI Compliance	S-116-732-2013 Category 6, ANSI/NEMA WC-66 Category 6
CAT-TR-19	Telecommunications Standards	ANSI/TIA-568-C.2 Category 6
CAT-TR-20	IEEE Specification	POE per 802.3af & POE+ per 802.3at-2009

#### 7.1.9 IR illuminator

S. No.	Nature of requirement	Minimum Requirement Specifications
IRI-TR-01	Range Distance	Minimum 200 Meters
IRI-TR-02	Adaptive illumination	10 to 80 degrees using lens; High sensitivity at Zero lux
IRI-TR-03	Power	Input 100-240V AC, or 12/24 V AC/DC, and automatic on/off operation
IRI-TR-04	Casing	IP66 rated / NEMA 4X vandal resistance
IRI-TR-05	Operating Condition	-5° to 50°C or better
IRI-TR-06	Certification	CE, FCC, RoHS
IRI-TR-07	Lighting	High Definition LED's
IRI-TR-08	Required Accessories	Power Supply, Mounting Clamps, U-bracket
IRI-TR-09	Support	The system should not be an end of life / end of service product

#### 7.1.10 Emergency Call Box with Panic Button

S. No.	Category	Minimum Requirement Specifications
ECB-TR-01	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment
ECB-TR-02	Connectivity	GSM/PSTN/Ethernet as per solution offered
ECB-TR-03	Sensors	For tampering/Vandalism
ECB-TR-04	Battery	Internal Battery with different charging options (Solar/Mains)
ECB-TR-05	Power	Automatic on/off operation
ECB-TR-06	Casing	IP-55 rated for housing
ECB-TR-07	Operating conditions	0° to 50°C

### 7.1.11 ANPR LPU (Inside Junction Box)

S. No.	Nature of requirement	Minimum Requirement Description
LPU.FRS.TR.01	Technical	Shall have minimum Quad Core CPU (4 physical CPU cores)
LPU.FRS.TR.02	Technical	Shall have minimum 64-bit architecture
LPU.FRS.TR.03	Technical	Shall have minimum 8 GB RAM (DDR3-1600 or above)
LPU.FRS.TR.04	Technical	Shall have minimum 500 GB Hard Disk
LPU.FRS.TR.05	Technical	Shall have Dedicated Gigabit network port per camera (MTU 9000 / jumbo frames), +1 LAN port
LPU.FRS.TR.06	Technical	Shall have capability to connect 4 cameras per LPU

### 7.1.12 Body Camera

S. No.	Nature of Requirement	Minimum Requirement Specifications
BC-TR-01	General	The Body Worn Camera System (BWCS) should consist of a single device comprising of a camera, rechargeable battery and recording unit. It should be able to capture clear high definition video & audio as well as take still photographs. It should be able to compress the video/audio files using appropriate non-proprietary algorithm and store it on a local drive.
BC-TR-02	Dimensions	The BWCS should be lightweight, of a small size and be comfortable to wear on the body. It can be mounted / installed on the shoulder or shirt front or shirt pocket etc. The mounting should be of an ambidextrous design and should keep the equipment stable.
BC-TR-03	Capture of video, audio and still photographs	The BWCS should be a point of view audio/video recording system capable of capturing audio/video/still photographs of what the officer is seeing.
BC-TR-04	Date and Time Stamping	The camera shall contain an embedded real-time clock which provides accurate date and time stamps on videos/ photographs.
BC-TR-05	Recording Resolution	The camera should encode video at resolution upto HD quality (1280 x 720 pixel or better).
BC-TR-06	Camera Sensor	The camera should capture video & photograph with a minimum of 1 megapixel sensor. It should also have capability of night mode recording.
BC-TR-07	Field of view of lens	100 degrees or better.
BC-TR-08	Display	Minimum 2" LCD colour Display
BC-TR-09	Replay	The device should be able to play the recorded audio/video/images on the screen.

S. No.	Nature of Requirement	Minimum Requirement Specifications
BC-TR-10	Compression	The camera must support MPEG-4 / H.264 (video) and MPEG-4/ MP2 (audio) compression algorithm and should offer the compression at upto 30 frames per second.
BC-TR-11	Storage	The BWCS shall support on-board storage via Solid State Storage or SD Card of 32 GB capacity (included). The on-board storage should be sufficient to record up to 08 hours at maximum resolution.
BC-TR-12	Battery	The BWCS should be supplied with an internal rechargeable Lithium battery. The battery should be of appropriate capacity to allow for continuous use including recording for up to 4 hours.
BC-TR-13	Battery recharge time	The battery recharge time from empty to full capacity should be not more than 3 hours.
BC-TR-14	Data Transfer	Each BWCS should be able to connect and upload data using a USB 2.0 port or better.
BC-TR-15	Configurations and Video Management	All configurations (including the adjustment of the real time clock) of the BWCS should be possible via a PC-based windows application. The management application should allow the user to backup and transfer data from one or multiple BWCS and also allow query for video/photograph on the basis of device, user, time, filename etc.
BC-TR-16	Battery charger	Each BWCS should be supplied with a separate charger.
BC-TR-17	Security features	The user should not be able to delete / edit / overwrite original video file/photograph. The deletion/uploading/ transfer of video/photograph on a PC should be possible only through the management software and should be administrator controlled. However, there should be an option of auto-overwriting on the basis of oldest-file-first-to-be-deleted, once the memory is full and further recording is being done.
BC-TR-18	Design	The BWCS should be water resistant, dust resistant, impact resistant and should be operable in normal steady rainfall (IP-55 or better). The BWCS should have an LED warning light which should remain 'On' when the camera is recording. It should also give an audible beep when the camera is switched on/ off and when the battery has become low etc.
BC-TR-19	Operating Temperature	0 to 55 degrees C.

S. No.	Nature of Requirement	Minimum Requirement Specifications
BC-TR-20	Night Vision	
BC-TR-20	Warranty	The BWCS should have a comprehensive onsite warranty (incl. battery) for 3 years.

### 7.1.13 Docking System

S. No.	Nature of Requirement	Minimum Requirement Specifications
DS-TR-01	Capacity	Min 10 slot chassis with battery charging
DS-TR-02	Connection	Single USB and Power connection
DS-TR-03	Functionality	Should be Capable to transfer data from device automatically to defined system when docked and simultaneously charge the device. Docking station for single device and 10 (for multiple device data transfer and charging at a time) both to be provided

## 7.2 Environment Sensor

### 7.2.1 Air Quality Monitoring Station

S. No.	Nature of requirement	Minimum Requirement Specifications
SE-TR-01	General	Should be ruggedized enough to be deployed in open air areas, on streets and parks
SE-TR-02	General	Should be able to read and report the following parameters: PM 10, PM 2.5, NO2, SO2, CO, O3, CO2,
SE-TR-03	Connectivity	Sensors should be able to connect through Fibre, USB, Ethernet, Wi-Fi, 2G, 3G 4G, LTE, LoRA connectivity mediums, whichever was feasible
SE-TR-04	Environmental Conditions	Enclosure shall be rugged weather proof IP65 rated and shall house the power modules, thermal management system, embedded PC and user configured Analyzer modules as well
SE-TR-05	Environmental Conditions	Environmental operating range shall be 0°C to +60°
SE-TR-06	General	The design shall be modular in nature which shall have the capability to add additional environmental sensors in the future into the enclosure
SE-TR-07	General	Data of all the environmental sensor shall be available on the same software interface
SE-TR-08	General	It shall be possible to remove or replace individual sensor modules without affecting the functioning of rest of the system
SE-TR-09	General	Data of all the environmental sensor shall be available on the same software interface

S. No.	Nature of requirement	Minimum Requirement Specifications
SE-TR-10	General	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod stand or a standalone pole

### 7.2.2 Carbon Mono Oxide (CO) Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
CO.TR.01	Range	Range of CO sensor shall be between 0 to 1000 PPM
CO.TR.02	Resolution	Resolution of CO sensor shall be 0.01 PPM or better
CO.TR.03	Lower Detectable Limit	Lower detectable limit of CO sensor shall be 0.040 PPM or better
CO.TR.04	Precision	Precision of CO sensor shall be less than 3% of reading or better
CO.TR.005	Linearity	Linearity of CO sensor shall be less than 1% of full scale or better
CO.TR.006	Response Time	Response time of CO sensor shall be less than 60 seconds
CO.TR.007	Operating Temperature	Operating temperature of CO sensor shall be 0°C to 60°C
CO.TR.008	Operating Pressure	Operating pressure of CO sensor shall be ±10%

### 7.2.3 Ozone (O3) Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
OZ.TR.001	Range	O3 Sensor shall have a range of at least 0-1000 PPB.
OZ.TR.002	Resolution	Resolution of O3 sensor shall be 10 PPB or better.
OZ.TR.003	Lower Detectable Limit	Lower detectable limit of O3 sensor shall be 10 PPB or better.
OZ.TR.004	Precision	Precision of O3 sensor shall be less than 2% of reading or better.
OZ.TR.005	Linearity	Linearity of O3 sensor shall be less than 1% of full scale.
OZ.TR.006	Response Time	Response time of O3 sensor shall be less than 60 seconds.
OZ.TR.007	Operating Temperature	Operating temperature of O3 sensor shall be 0°C to 60°C.
OZ.TR.008	Operating Pressure	Operating pressure of O3 sensor shall be ±10%.

#### 7.2.4 Nitrogen Dioxide (NO<sub>2</sub>) Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
NO <sub>2</sub> .TR.001	Range	NO <sub>2</sub> Sensor shall have a range of at least 0-10 PPM.
NO <sub>2</sub> .TR.002	Resolution	Resolution of NO <sub>2</sub> sensor shall be 0.001 PPM or better.
NO <sub>2</sub> .TR.003	Lower Detectable Limit	Lower detectable limit of NO <sub>2</sub> sensor shall be 0.001 PPM or better.
NO <sub>2</sub> .TR.004	Precision	Precision of NO <sub>2</sub> sensor shall be less than 3% of reading or better.
NO <sub>2</sub> .TR.005	Linearity	Linearity of NO <sub>2</sub> sensor shall be less than 1% of full scale.
NO <sub>2</sub> .TR.006	Response Time	Response time of NO <sub>2</sub> sensor shall be less than 60 seconds.
NO <sub>2</sub> .TR.007	Operating Temperature	Operating temperature of NO <sub>2</sub> sensor shall be 0°C to 60°C.
NO <sub>2</sub> .TR.008	Operating Pressure	Operating pressure of NO <sub>2</sub> sensor shall be ±10%.

#### 7.2.5 Sulphur Dioxide (SO<sub>2</sub>) Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
SO <sub>2</sub> .TR.001	Range	SO <sub>2</sub> Sensor shall have a range of at least 0-20 PPM.
SO <sub>2</sub> .TR.002	Resolution	Resolution of SO <sub>2</sub> sensor shall be 0.001 PPM or better.
SO <sub>2</sub> .TR.003	Lower Detectable Limit	Lower detectable limit of SO <sub>2</sub> sensor shall be 0.009 PPM or better.
SO <sub>2</sub> .TR.004	Precision	Precision of SO <sub>2</sub> sensor shall be less than 3% of reading or better.
SO <sub>2</sub> .TR.005	Linearity	Linearity of SO <sub>2</sub> sensor shall be less than 1% of full scale.
SO <sub>2</sub> .TR.006	Response Time	Response time of SO <sub>2</sub> sensor shall be less than 60 seconds.
SO <sub>2</sub> .TR.007	Operating Temperature	Operating temperature of SO <sub>2</sub> sensor shall be 0°C to 60°C.
SO <sub>2</sub> .TR.008	Operating Pressure	Operating pressure of SO <sub>2</sub> sensor shall be ±10%.

#### 7.2.6 Carbon Dioxide (CO<sub>2</sub>) Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
CO <sub>2</sub> .TR.001	Range	CO <sub>2</sub> Sensor shall have a range of at least 0-5000 PPM.
CO <sub>2</sub> .TR.002	Resolution	Resolution of CO <sub>2</sub> sensor shall be 1 PPM or better.

S. No.	Nature of requirement	Minimum Requirement Specifications
CO2.TR.003	Lower Detectable Limit	Lower detectable limit of CO2 sensor shall be 10 PPM or better.
CO2.TR.004	Precision	Precision of CO2 sensor shall be less than 3% of reading or better.
CO2.TR.005	Linearity	Linearity of CO2 sensor shall be less than 2% of full scale.
CO2.TR.006	Response Time	Response time of CO2 sensor shall be less than 60 seconds.
CO2.TR.007	Operating Temperature	Operating temperature of CO2 sensor shall be 0°C to 60°C.
CO2.TR.008	Operating Pressure	Operating pressure of CO2 sensor shall be ±10%.

#### 7.2.7 PM10 Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
PM10.TR.001	Range	Range of PM10 shall be 0 to 450 micro gms / cu.m or better.
PM10.TR.002	Lower Detectable Limit	Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3.
PM10.TR.003	Accuracy	Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading).
PM10.TR.004	Flow Rate	Flow rate shall be 1.0 LPM or better.
PM10.TR.005	Operating Temperature	Operating temperature of the sensor shall be 0°C to 60°C.
PM10.TR.006	Operating Pressure	Operating pressure of the sensor shall be ±10%.

#### 7.2.8 PM2.5 Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
PM10.TR.001	Range	Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better.
PM10.TR.002	Lower Detectable Limit	Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3.
PM10.TR.003	Accuracy	Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading).
PM10.TR.004	Flow Rate	Flow rate shall be 1.0 LPM or better.
PM10.TR.005	Operating Temperature	Operating temperature of the sensor shall be 0°C to 60°C.
PM10.TR.006	Operating Pressure	Operating pressure of the sensor shall be ±10%.

### 7.2.9 Noise Sensor

S. No.	Nature of requirement	Minimum Requirement Specifications
NS.TR.001	General	Noise sensor shall detect the intensity of the ambient sound in a particular area.
NS.TR.002	General	Noise Sensors shall be installed for the outdoor applications.
NS.TR.003	Range	Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA.

### 7.3 Fleet Tracking Unit

S. No.	Nature of requirement	Indicative Requirement Description
VTU.TR.001	Frequency	850MHz/900MHz/1800MHz/1900MHz Quad band
VTU.TR.002	GPRS	Class 12
VTU.TR.003	GPS/ GSM Antenna	Built-Inside Unit, Option of External Antenna
VTU.TR.004	GPS Modem	Multi-GNSS GPS and GLONASS with AGPS support
VTU.TR.005	Positioning accuracy	Less than 10 meter
VTU.TR.006	Tracking Sensitivity	-165 dBm
VTU.TR.007	Acquisition Sensitivity	-148 dBm
VTU.TR.008	TTFF(Open Sky)	Cold Start: <32 seconds , Hot Start : < 1 Seconds
VTU.TR.009	Operating Voltage	8-40VDC
VTU.TR.010	Operating Temperature & Humidity	-20 to +60 degree centigrade , 5-95% RH
VTU.TR.011	LED indicators	GPS Status , GSM Status , Power Status
VTU.TR.012	Shock Test Certification	40g, 11ms, 3 pos/neg per axis, 18 terminal peak saw tooth pulses 75g, 11ms, 2 pos/neg per axis, 12 terminal peak saw tooth pulses
VTU.TR.013	Vibration Certification	10Hz to 2000Hz, 3 Axes, 1 Hour/Axis
VTU.TR.014	Casing	ABS , UV Stabilized
VTU.TR.015	IP Rating	IP 67
VTU.TR.016	Battery Backup	Lithium ion rechargeable , 6 Hours backup , 1100 mAH minimum , Protection Circuit and Battery temperature monitoring
VTU.TR.017	Transport and Application Protocol Support	NMEA 0183 , TCP , HTTP , MQTT , SMS , SMTP
VTU.TR.018	Security	TLS 1.2 with device authentication mechanism
VTU.TR.019	Ports	USB 2.0 and RS232 Support

S. No.	Nature of requirement	Indicative Requirement Description
VTU.TR.020	Analog Input	0-10V , Remote Battery Monitoring
VTU.TR.021	Digital Inputs	Minimum 3 (Odometer Pulse , Ignition Status, Spare)
VTU.TR.022	Digital Outputs	Minimum 2
VTU.TR.023	Accelerometer	3 Axis , +/- 16g , 12 Bit
VTU.TR.024	Geo fencing	Supported
VTU.TR.025	Storage	15000 Logs in device, synced with server in FIFO mode, device logs shall be deleted only after confirmation of reception from server
VTU.TR.026	Over the Air Firmware Upgrade	Supported over GPRS network
VTU.TR.027	SIM card	Micro Sim Slot
VTU.TR.028	Protection	Reverse Battery , Transients , EMI/ EMC
VTU.TR.029	Battery Conservation	The system shall support saving battery power in sleep mode when vehicle is at rest by reducing frequency of location transmissions.

## 7.4 Waste Water Sensor

### 7.4.1 Multi-Parameter Smart Controller (Micro-Station) for COD, BOD, TOC, TSS, pH, DO, NH4-N, Temperature, Oil and Grease parameters

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-01.1	General	Micro-Station/Controller shall have the latest features of highly advanced Multi Parameter Controller having capability of handling at least 4 Sensors in a single controller configuration and more as and when required with Sensor ID recognition and high EMC interference immunity
WQSP -TR-01.2		It shall be supplied with Modular Plug and Play system in which sensor can be added/changed at any time and at any location
WQSP -TR-01.3		It shall be supplied with Sensor ID recognition feature with high interference immunity.
WQSP -TR-01.4		The device shall be with easy Panel Mounting with required accessories.
WQSP -TR-01.5		Controller shall have the capability to be operated as Controller (having programmability feature) or just a terminal (that can display the data without any way to make changes).

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-01.6		The Micro-Station shall be able to power all the sensors and terminals or accessories attached to it without having to need any additional power sources in the system for increased protection against lightening and possible electromagnetic interference
WQSP -TR-01.7	Display	The device shall be supplied with large graphic display with backlight. Display shall be with improved reading precision through special backlit graphic display
WQSP -TR-01.8		Input voltage: 220 VAC and 50 Hz
WQSP -TR-01.9		Output: Galvanically separated current outputs (0/4-20 mA) that can be assigned arbitrarily, RJ45 Ethernet availability, USB-interface for data transfer, upgrading firmware etc.
WQSP -TR-01.10	Electrical	The system should start automatically after the power is reset to the system (in case of power failure). The system should have Service mode for cleaning/calibration/maintenance activities.
WQSP -TR-01.11		The controller shall store the sensor configurations and calibrations
WQSP -TR-01.12		The controller shall have Logbook to record the data
WQSP -TR-01.13		The supplier shall provide the firmware update free of cost as and when they are available for the life time of the system
WQSP -TR-01.14	Interfaces	External interfacing with IEG (Intelligent Edge Gateway) using Modbus interfaces.
WQSP -TR-01.15	Measuring Parameters	COD, BOD, TOC, TSS, pH, Temperature, DO, Conductivity, NH4-N, Oil & Grease etc.
WQSP -TR-01.16	Operating Temperature	Ambient Operating temperature: -20 °C to 55 °C , Storage temperature: -10 °C ... 60 °C
WQSP -TR-01.17	Process Connection	1" PVC type process Connection
WQSP -TR-01.18	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-01.19	Protection	Electromagnetic Compatibility: EN 61326, Class B; FCC Class A, EMC for indispensable operation
WQSP -TR-01.20		Integrated Lightening protection, Protection Rating IP 66

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-01.21	Calibration	Timely Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period.
WQSP -TR-01.22	Certification	CE/UL/EN/BIS
WQSP -TR-01.23	Cables	Necessary cables for power, communication and data
WQSP -TR-01.24	Accessories and Laying	Bidder shall provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.

#### 7.4.2 Sensor Probe for BOD/COD/TOC/TSS

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-02.1	General	The probe shall be a Multi parameter Probe. It shall be continuously Effluent Monitoring of BOD, COD, TOC, TSS with UV-Vis Full Spectrum Technology.
WQSP -TR-02.2		It shall be ideally for Waste Water measurements in Open Channel with direct In-Situ measurement along with floating type arrangement using SS chain.
WQSP -TR-02.3		It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation
WQSP -TR-02.4		The device shall be with easy Mounting without Clogging
WQSP -TR-02.5		The Sensor should provide compensation of interferences by evaluation of the whole measured spectrum.
WQSP -TR-02.6	Measuring Principle	It shall have the UV-Vis Spectrometry principle for measurement over the total Range (190 - 720 nm)
WQSP -TR-02.7	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-02.8		The probe shall be supplied with Integrated cleaning system
WQSP -TR-02.9	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration. Timely

S. No.	Nature of requirement	Minimum Requirement Specifications
		Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period
WQSP -TR-02.10	Measuring Parameters	BOD, COD, TOC, TSS
WQSP -TR-02.11	Accuracy	±2%
WQSP -TR-02.12	Operating Temperature	0° C to 50° C
WQSP -TR-02.13	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface
WQSP -TR-02.14	Protection	The Probe shall support the IP68 protection standard
WQSP -TR-02.15		The device shall have the conformity to EMC and Safety with EN 61326-1, EN 61326-2-3 and EN 61010-1 standards
WQSP -TR-02.16		The sensor should be completely reagent free for operation.
WQSP -TR-02.17	MOC	The MOC must be Titanium Material or equivalent to sustain the sensor in highly corrosive wastewater environment.
WQSP -TR-02.18	Light Source	Xenon Flash Lamp
WQSP -TR-02.19	Measuring Range	COD: 0 - 20000 mg/l BOD: 0 - 8000 mg/l TOC: 0 - 20000 mg/l TSS: 0 - 4500 mg/l However, SI shall conduct the site survey and range of the probes shall be according to the site survey / Lab Report.
	Accessories and laying	Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.

#### 7.4.3 Sensor Probe for DO (Dissolved Oxygen)

S. No.	Nature of requirement	Minimum Requirement Specifications
DO probe		
WQSP -TR-05.1	General	The probe shall be a Multi-parameter Probe
WQSP -TR-05.2		It shall be used ideally for Open Canal (Floating Type)

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-05.3		It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation
WQSP -TR-05.4		Long term stable and maintenance free operation
WQSP -TR-05.5	Resolution	0.01 mg/l O <sub>2</sub>
WQSP -TR-05.6	Measuring Principle	Mounting and Measurement shall be directly in the media or in a flow cell (Monitoring Station)
WQSP -TR-05.7	Cleaning	The probe shall have the optical/fluorescence measurement principle
WQSP -TR-05.8		The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-05.9	Calibration	Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC
WQSP -TR-05.10	Measuring Parameters	Long term stable and maintenance free operation
WQSP -TR-05.11	Accuracy	The probe shall be factory pre-calibrated and with local multi-point calibration
WQSP -TR-05.12	Operating Temperature	Dissolved Oxygen
WQSP -TR-05.13	Interface to Scanner	±1%
WQSP -TR-05.14	Protection	0° C to 60° C
WQSP -TR-05.15		The probe shall be interface with Scanning terminal using RS 485 interface

#### 7.4.4 Sensor Probe for Nitrate (NO<sub>3</sub>-N) and Ammonical Nitrogen (NH<sub>4</sub>-N)

S. No.	Nature of requirement	Minimum Requirement Specifications
<b>NH4-N</b>		
WQSP -TR-03.1		The probe shall be a Multi parameter Probe with Adjustable open path length
WQSP -TR-03.2		It shall be ideally for Waste Water Treatment Process
WQSP -TR-03.3	General	It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation
WQSP -TR-03.4		ISE Refurbishment for easy maintenance

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-03.5		Mounting and Measurement shall be directly in the media or in a flow cell (Monitoring Station)
WQSP -TR-03.6	Measuring Principle	It shall have the Ion selective electrodes without potassium compensation for measurement
WQSP -TR-03.7	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-03.8		The probe shall be supplied with Integrated cleaning system
WQSP -TR-03.9	Calibration	The probe shall be Factory calibrated with optional In-Situ calibration for improved accuracy. Timely Calibration of the instrument based on pre-defined time schedule shall be done by the MSI during AMC Period
WQSP -TR-03.10	Measuring Parameters	NH4-N, NO3-N
WQSP -TR-03.11	Accuracy	±3%
WQSP -TR-03.12	Operating Temperature	0° C to 60° C
WQSP -TR-03.13	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface
WQSP -TR-03.14	Protection	The Probe shall support the IP68 protection standard
WQSP -TR-03.15		Conformity to EMC with EN 50081-1, EN 50082-1, EN 60555-2, EN 60555-3 & to safety with EN 61010-1 standards
WQSP -TR-03.16	Cable	The Sensor cable supplied along with the sensor shall be 15 Meters and of Sea Water version so that it's not affected by acids and presence of highly corrosive media in sample.
WQSP -TR-03.16	Measuring Range	0.1 ...1000 mg/l NO3-N 0.1 ...1000 mg/l NH4-N However, SI shall conduct the site survey and range of the probes shall be according to the site survey / Lab report.

#### 7.4.5 Sensor Probe for pH and Temperature

S. No.	Nature of requirement	Minimum Requirement Specifications
pH and Temperature Probe		
WQSP -TR-05.1	General	The probe shall be a Multi-parameter Probe
WQSP -TR-05.2		It shall be ideally for Waste Water monitoring Process in an Open Channel (Floating Type)
WQSP -TR-05.3		It shall have MoC (Material of Construction) such as Titanium Material or Stainless Steel to sustain the sensor in highly corrosive wastewater environment for long term stable and maintenance free operation
WQSP -TR-05.4		Long term stable and maintenance free operation
WQSP -TR-05.5		Integrated temperature measurement and compensation shall be provided in the pH sensor.
WQSP -TR-05.6		The pH sensor should have Galvanically separated input. Temperature Sensor shall be integrated in the pH sensor.
WQSP -TR-05.7	Cleaning	The pH combination electrodes shall be required very little maintenance and there should be no electrolyte replacement (Reagent Free).
WQSP -TR-05.8		The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-05.9	Calibration	Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC
WQSP -TR-05.10	Measuring Parameters	Probe shall use the Electro Chemical measuring principles to measure the pH and Temperature.
WQSP -TR-05.11	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration
WQSP -TR-05.12	Measuring Range	Measuring Range: pH: 0.00- 14.00 at least considering the waste water environment Measuring Range Temperature: -5 to 60° C
WQSP -TR-05.13	Operating Temperature	Temp Compensation: -5 to 50° C
WQSP -TR-05.14	Accuracy	±1%
WQSP -TR-05.15	Interface	The probe shall be interface with Scanning terminal using RS 485 interface

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-05.16	Sensor Cable	The Sensor cable supplied along with the sensor has to be 15 Meters and of Sea Water version so that it's not affected by acids and presence of highly corrosive media in sample.
WQSP -TR-05.17	Measuring Range	Measuring Range: pH: 0.00- 14.00 units at least considering the wastewater environment Temperature Measuring: -5 to 60 Deg C
WQSP -TR-05.19	Accessories Laying	Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.

#### 7.4.6 Probe for Oil & Grease Analyser (Open Channel, Floating Type)

S. No.	Nature of requirement	Minimum Requirement Specifications
Oil & Grease		
WQSP -TR-06.1	General	The probe shall be used to measure Oil and Grease in waste water using UV fluorescence technology.
WQSP -TR-06.2		It shall be ideally for Waste Water Treatment Process
WQSP -TR-06.3		It shall have Long term stable and maintenance free operation
WQSP -TR-06.4	Housing	The Probe shall be supplied with stainless steel, Titanium housing material
WQSP -TR-06.5	Mounting	The probe shall be vertically mounted
WQSP -TR-06.6	Measuring Principle	The probe shall have the UV fluorescence (254 - 360 nm) measurement principle
WQSP -TR-06.7	Cleaning	The probe shall have the Automatic cleaning facility with compressed air or brush or using Ultrasonic methods whichever is best suitable
WQSP -TR-06.8		The probe shall be supplied with Integrated cleaning system
WQSP -TR-06.9	Calibration	The probe shall be factory pre-calibrated and with local multi-point calibration. Timely Calibration of the instrument based on the pre-defined time schedule shall be done by the MSI during AMC
WQSP -TR-06.10	Measuring Parameters	Oil & Grease

S. No.	Nature of requirement	Minimum Requirement Specifications
WQSP -TR-06.11	Limit of Detection	1 µg/L
WQSP -TR-06.12	Operating Temperature	0° C to 60° C
WQSP -TR-06.13	Interface to Scanner	The probe shall be interface with Scanning terminal using RS 485 interface
WQSP -TR-06.14	Protection	The Probe shall support the IP68 protection standard
WQSP -TR-06.15		Conformity to EMC with EN 50130-4, 61000 - 6- 1 standards
WQSP -TR-06.16	Accessories and Laying	Bidder to provide wiring, piping, cable tray and accessories required to make a completely integrated system. Provide all components, piping, wiring, accessories, cable tray and labour required for a complete and integrated system without any extra cost to tendering authority.

#### 7.4.7 IEG with integrated 3G/4G communication capabilities with Cable and Other Accessories

S. No.	Nature of requirement	Minimum Requirement Specifications
Multi-Channel Transmitter / Remote Terminal Unit		
IEG -TR-01.1	General	Industrial grade IEG with Analog input channels shall be supplied for integrating various quality Analysers / controllers to monitor the waste water quality parameters.
IEG -TR-01.2		The device shall have interfaces to integrate quality analysers/controllers using Modbus RTU interfaces for upstream communication.
IEG -TR-01.3		It shall have be hot plug and play device with minimum configuration. It shall have inbuilt real-time clock with synchronization from GSM network
IEG -TR-01.4		The device shall have easy Extension and Adaptation facility
IEG -TR-01.5	Environmental	The supplied unit shall perform the vibration tests producing certificates from National standard Laboratories
IEG -TR-01.6		EMI / EMC certified
IEG -TR-01.7		The device shall be suitable for hazardous environment and shall be IP 67 standard of protection
IEG -TR-01.8	Mechanical	Din Rail mounted with Input module

S. No.	Nature of requirement	Minimum Requirement Specifications
IEG -TR-01.9		The device shall be supplied with fixtures for Pipe mounting / wall mounting / Panel mounting possibilities.
IEG -TR-01.10	Electrical	Power Supply: 220V AC
IEG -TR-01.11		IP66 to EN 60529/09.2000 Complies with NEMA 4.
IEG -TR-01.12		Accuracy: 0.1%
IEG -TR-01.13		Span: > 0 to 20 mA
IEG -TR-01.14		Resolution of current inputs: < 5 µA
IEG -TR-01.15		Nominal Input Current: Max. 8 mA
IEG -TR-01.16		Signal Characteristic : Linear
IEG -TR-01.17		Internal Resistance: Non-Linear
IEG -TR-01.18		The supplied unit shall have over voltage and Lightning protection feature
IEG -TR-01.19		Easy remote configuration and software update facilities
IEG -TR-01.20		Inbuilt plug-in I/O support
IEG -TR-01.21		Electrical Safety : IEC 61010-1, Class I equipment Low voltage: overvoltage category II protection
IEG -TR-01.22		Memory: 16 MB flash , 2 MB RAM
IEG -TR-01.23	Communication	Communication shall be over Modbus / Ethernet IP/ Any Open IoT protocols such that it shall be able to send data to centralized application server (OWQMS) over GSM / GPRS network using 3G/4G enabled inbuilt modems.
IEG -TR-01.24		Interfaces: RS485 half-duplex, 8kV air discharge protection, 4kV,ESD Protection Contact
IEG -TR-01.25		The device shall be integrated with Central applications for waste water quality data analysis

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

S. No.	Nature of requirement	Minimum Requirement Specifications
FE-Req.01	Built	The Outdoor Utility Cabinet shall be constructed with a front sheet steel door with Locking system to ensure the security of the cabinet. Side and Wall Panels shall be with fixing bolts internal to the cabinet. The Cabinet should have the required frames to mount the required components like Field equipment such as IEG / DCU / Gateways / MCT / Analysers, Power supply Equipment, Networking Equipment, LIU, battery, etc.

FE-Req.02	Utility & IP rating	Should be Made for 24/7/365 Outdoor Applications; The Utility Cabinet shall be IP67 or better rated with built-in air-cooling system. Field Enclosure design should ensure to keep the operating temperature / ambient temperature within suitable operating range 20° C to 55° C for equipment's and should also avoid condensation, corrosion, intentional water splash and dust intake.
FE-Req.03	Size	The cabinet has to be provided of size suitable for the mounting of the associated network devices, power, UPS and battery components securely and safely within the cabinet.
FE-Req.04	Power Slot	PDU type should be as per actual requirement as per Indian standards.
FE-Req.05	Cable Management	Proper cable management should be provided.

## 7.5 Network Backbone

### 7.5.1 Electric Meter

S. No.	Nature of requirement	Minimum Requirement Description
ELEM.TR.01	Voltage	Reference Voltage 230 volt (P-N), +20% to -40% Vref. However the meter should withstand the maximum system voltage.
ELEM.TR.02	Display	a) LCD (Seven digits) b) Height: 8 mm X 5 mm min. c) Pin Type d) Viewing angle min. 120 degrees
ELEM.TR.03	Display parameters	LCD test, date & time, cumulative KWH, cumulative KVAH & KVArH, MD in KW & KVA, PF, V, I and Neutral current (All the energies are without decimal.)
ELEM.TR.04	Power factor range	Zero lag -unity- zero lead
ELEM.TR.05	Power Consumption	1. Normal Operation As per IS16444 2. Relay operation As per IS16444 3. Communication As per IS16444 4. Relay operation + communication As per IS16444
ELEM.TR.06	Starting current	0.2 % of Ib
ELEM.TR.07	Frequency	50 Hz with (+ or -) 5% variation
ELEM.TR.08	Test Output Device	Flashing 02 nos. separate LED visible from the front for testing of kWh and kVARh in field also.
ELEM.TR.09	Billing data	a) Meter serial number, Date and time, KWH, KVAH, KVArH, MD in KW and KVA, No. of tamper counts, tamper occurrence with date & time, tamper restoration date & time with snap shots. History of KWH, KVAH, KVArH & MD with occurrence details for last 6 months along with TOD readings. b) All the above parameters (namely KWH, KVAH, KVArH, MD in KW and KVA) are meter readings. c) All these data shall be accessible for reading, recording by downloading through optical port with CMRI, HES & Laptop computers at site.

S. No.	Nature of requirement	Minimum Requirement Description
		d) Meter should be configurable to be used in bidirectional i.e. Net metering mode (import/export and total energy in separate register required).
ELEM.TR.10	MD Registration	Meter shall store MD in every 30 min. period along with date & time. At the end of every 30 min, new MD shall be compared with previous MD and store whichever is higher and the same shall be displayed. It shall be preferred that MD is computed using separate counter rather by difference of initial and final energy counter.
ELEM.TR.11	Auto Reset of MD	Auto reset date for MD shall be indicated at the time of finalizing GTP. Default re-setting date is 00:00 hrs. 1st of every month.
ELEM.TR.12	TOD metering	Meter shall be capable of doing TOD metering for KWH, KVARH, KVAH and MD in KW and KVA with 6 time zones and three tariff zones (programmable on site through CMRI & Remote)
ELEM.TR.13	Load survey	30 min integration period, load profile of KW, KVA , voltage and current, for min. 35 days
ELEM.TR.14	Diagnostic feature	Self-diagnostic for time, calendar, RTC battery all display segments and NVM.
ELEM.TR.15	Security feature	Programmable facility to restrict the access to the information recorded at different security level such as read communication, communication write etc. Proper security at endpoint as well as network level shall be present to prevent unauthorized hacking of the end point or the network itself.
ELEM.TR.16	Software & communication compatibility	a) Optical port b) CMRI support It shall be possible to read the smart meter using CMRI thru the local communication port (Optical or RS232). It shall be possible to upload the meter readout file from CMRI to HES. CMRI support

S. No.	Nature of requirement	Minimum Requirement Description
		<p>shall be required for the following field scenarios:</p> <ul style="list-style-type: none"> <li>i. Meter data from field on the communication failed cases for billing purpose.</li> <li>ii. In case meter is damaged and not reachable by HES, then CMRI data is crucial for further analysis.</li> <li>c) Communication Facility - Communication technology shall be GPRS/3G or upward as specified in IS16444 Part-1.</li> <li>d) Communication Protocol</li> </ul> <p>Meter Protocol: Meter shall support DLMS as per IS15959 Part2</p> <ul style="list-style-type: none"> <li>e) The Meter manufacturer shall supply software required for local (CMRI) &amp; remote (AMI) connectivity including required training to use the software free of cost.</li> <li>f) Key Management and Security Feature should be as per IS 15959.</li> <li>g) Optical port to transfer the data locally through CMRI &amp; remote through GSM / GPRS/2G/3G or upward to the HES.</li> <li>h) It shall be possible to reconfigure the meters for TOD Tariff, DIP (Demand Integration period), billing date etc. through proper authentication process locally through CMRI/ remotely.</li> <li>i) Meter Serial no and consumer CA nos. shall be used for tagging of all data of the meters in all database (at HES level).</li> <li>j) At any point of time, the pre -paid meter at site shall be configurable from remote to a Post-paid meter and vice -versa or Net meter as desired, by BRPL on receipt of request from the customer.</li> </ul>
ELEM.TR.17	Memory	Non-volatile memory independent of battery backup, memory should be retained up to 10 year in case of power failure
ELEM.TR.18	Climatic conditions	<ul style="list-style-type: none"> <li>a) The meter should function satisfactorily in India with temperature ranging from 0 - 60°C and humidity up-to 96%.</li> <li>b) Also refer IS: 13779 for climatic conditions.</li> </ul>

S. No.	Nature of requirement	Minimum Requirement Description
		c) Meter should be compatible for Indoor and Outdoor usage
ELEM.TR.19	Calibration	Modification in calibration shall not be possible at site by any means.
ELEM.TR.20	Battery	In case battery removal or total discharge same should not affect the working & memory of the meter.
ELEM.TR.21	KVAh definition	KVAh is computed based on KVArh and KWH value. If PF=1, or leading, then KVAh = KWH. At no instance KVAh < KWh.
ELEM.TR.22	Communication port	<p>A. Optical Port: Meter shall have optical communication port Optical sensor should be provided @100% qty of tender qty.</p> <p>B. The length of cable shall be 1 meter, terminated on female type DB-9 connector and should be suitable for smart meters data download through CMRI.</p> <p>C. It should have a life of 5 years both meter and optical sensor should have Mechanical arrangement, so as sensor can be fitted on meter without any tool and without any compromise on alignment and sensitivity.</p> <p>D. Wireless GPRS/3G Module / Port (GPRS/3G module for integration with HES/MDAS) Wireless module/port shall have provision for cover which can be sealed.</p>
ELEM.TR.23	Event logging and Phase diagram	Nomenclature used for any event logging/ flags/ parameters/ alarms shall be ease in understanding and shall be mutually decided by BSES. The same shall be convertible to CDF for further integration with BSES SAP system. It shall also be possible to convert to CSV/ ASCII/ XML format from HES/MDAS.
ELEM.TR.24	Real Time Clock	<p>a) A real time clock is required in meter, which maintains time and date</p> <p>b) The time shall be derived from an internal quartz crystal. Drift in time shall not be more than <math>\pm 5</math> minutes/year at a reference temperature of <math>27^{\circ}\text{C}</math>.</p>

S. No.	Nature of requirement	Minimum Requirement Description
		c) Time synchronization: Meter RTC shall be corrected automatically by HES/MDAS RTC in case found drift by more than ±2 minutes

### 7.5.2 Industrial grade Field Layer-2 FE 8 port POE Switch

S.No	Naturement of Requirement	Minimum Specifications
IGF8.TR.01	General Features	The switch should be Industrial Grade ruggedized in nature that provides minimum 8 x 10/100 BaseT access ports & 4xGE combo uplink ports. Switch should be supplied with required ruggedized Transceivers as per solution
IGF8.TR.02		Switch should have minimum 120W PoE power available or extra power injector should be provided in the junction box
IGF8.TR.03		The switch should have non-blocking wire-speed architecture with support for both IPv4 & IPv6 from day one with wire-rate
IGF8.TR.04		Should support minimum 10Gbps or more switching throughput
IGF8.TR.05		The switch should support backup storage drives, which will store the last known configuration of the switch, in the case of hardware failure and replacement. Reinserting the storage drive should restore the switch to original working condition without any manual intervention.
IGF8.TR.06		Switch must support Ethernet CFM / CFM (IEEE 802.1ag) and Uni-Directional Link Detection (UDLD) from day 1
IGF8.TR.07	Layer 2 Features	802. 1Q VLAN on all ports with minimum 16k MAC address
IGF8.TR.08		Spanning Tree Protocol as per IEEE 802.1d, ring protection protocol like REP or equivalent
IGF8.TR.09		Should support Jumbo frames up to 9000 bytes & Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
IGF8.TR.10		The switch should support IGMP v1/v2/v3 & up to 1000 IGMP groups as well as IGMP snooping & IGMP filtering. Should also support MLD v1/v2.
IGF8.TR.11	Layer 3 Features	Static, Inter-VLAN routing must be enabled from day one

S.No	Naturement of Requirement	Minimum Specifications
IGF8.TR.12		The switch should support Dynamic Routing - RIPv1/v2, OSPF for both IPv4 & IPv6, PBR, network address translation etc. protocol by enabling/upgrading the license as & when required.
IGF8.TR.13	Quality of Service (QoS)	Switch should support classification and scheduling as per IEEE 802.1P on all ports with minimum four egress queues per port
IGF8.TR.14		The switch should provide traffic shaping and rate limiting features for specified Host, network, Applications etc.
IGF8.TR.15		The switch should support ACLs, Extended IP ACLs, support RADIUS and TACACS+ for access restriction and authentication.
IGF8.TR.16	Security Features	Should support a mechanism to shut down Spanning Tree Protocol Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.
IGF8.TR.17		Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard, DHCP Snooping, DHCP Option 82, Dynamic ARP Inspection (DAI), IP Source Guard, Network Address Translation, BPDU Guard, Port-Security, DHCP Snooping, 802.1x, 802.1AE, MAC Authentication Bypass, 802.1x Multi-Domain Authentication, Storm Control
IGF8.TR.18	Management Features	The switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
IGF8.TR.19		Support for Automatic Quality of Service or equivalent for easy configuration of QoS features for critical applications.
IGF8.TR.20		Switch should support , FTP/TFTP
IGF8.TR.21	Mechanical Conditions:	Temperature: -5 to +70°C
IGF8.TR.22		Operating relative humidity: 5% to 95% no condensing
IGF8.TR.23		Protection Class -minimum IP 30, NEMA TS-2
IGF8.TR.24	Certifications	Switch should be EN 55022A Class A, VCCI Class A, KN22/CISPR 32 certified
IGF8.TR.25		The switch should support CIP Ethernet/IP, IEEE 1588 PTP and NTP to PTP translation.
IGF8.TR.26		EMC interface immunity:
IGF8.TR.27		Switch should be EN55024, EN 61000-4-2 Electro Static Discharge, EN 61000-4-5 Surge, EN 61000-4-8 Power Frequency Magnetic Field, EN 61000-4-11 AC Power Voltage

### 7.5.3 Industrial grade Field Layer-2 FE 16 port POE Switch

S. No.	Specification
1	The switch should provide Minimum 16 port 10/100 Mbps FE ports and 2 GE SFP uplinks Ports. Should be proposed with ruggedized transceivers as per solution.
2	802.1Q VLAN on all ports with support for minimum 500 active VLANs and minimum 4K Mac addresses
3	Switch should have minimum 120W PoE power available or extra power injector should be provided in the junction box
3	Spanning Tree Protocol as per IEEE 802.1d, 802.1s and 802.1w
4	Should support Improved resiliency with the support of Resilient Ethernet Protocol (REP) or equivalent for ring topology which should provide 50ms ring convergence
5	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
6	Switch should support IGMP v1/v2/v3 as well as IGMP snooping and minimum 250 IGMP Multicast Groups
7	The switch should support Dynamic Routing - RIP , OSPFv3 etc. protocol by enabling/upgrading the license as & when required and should be included static routing from day one
8	Switch should support non-blocking throughput and 1500 IPv4 & IPv6 routes
9	Switch must have Uni-Directional Link Detection (UDLD) feature
10	Switch should support classification and scheduling as per IEEE 802.1P
11	Switch should support strict priority queuing or Policing or equivalent to guarantee that the highest-priority packets are serviced ahead of all other traffic.
12	The switch should support following IPv6 Features: 128-Bit Wide Unicast Addresses, DNS for IPv6, ICMPv6, Neighbour Discovery, IPv6 Stateless Auto-configuration and Duplicate Address Detection, SNMP and Syslog Over IPv6, SSH/HTTP over IPv6 , HTTP over IPv6
13	RoHS Compliant, IEEE 1588v2 hardware ready - Precision Time Protocol, IEEE 802.3af, 802.3at, NTP compliant , RSPAN
14	Operating Temperature 0 C to +70C with fanless Enclosure
15	Relative Humidity of 5% or 95% Non-condensing
16	Must have EN 61000-6-1 Light Industrial EN 61000-6-2 Industrial EN 61000-6-4 Industrial EN 61326 Industrial Control EN 61131-2 Programmable Controllers
17	Must support FCC 47 CFR Part 15 Class A / FCC Part 15B, Class A EN 55022A Class A/ EN55032 Class A AS/NZS CISPR 22 Class A / CISPR 32

### 7.5.4 Junction Box 1 KVA (Outdoor Utility Cabinet)

S. No.	Nature of requirement	Minimum Requirements
JNB.TR.01		Out Door Cabinet with Pole Mount provision

S. No.	Nature of requirement	Minimum Requirements
JNB.TR.02	Mechanical Structure	Material - Galvanized Iron (GI) Sheet
JNB.TR.03		Thickness - Enclosure structure using 1.6 mm
JNB.TR.04		Foot plinth panel sheet minimum 3mm
JNB.TR.05	Ingress Protection	IP 55 Rated
JNB.TR.06	Colour	Colour - Grey / Relevant
JNB.TR.07	Coating thickness	Powder coating thickness between 70 to 120 micron Finish
JNB.TR.08	Cables	Cable management must be ensure proper path for AC supply
JNB.TR.09	Cable Entry	Cable entry on side bottom/Side wall through cable glands of PVC material to ensure rain water protection.
JNB.TR.10	Cooling	Forced air cooling to maintain approx. T < 10 Degree
JNB.TR.11	Filter	Removable and washable type pleated filters with aluminium wire mesh protection on both sides.
JNB.TR.12	Earthing	Diagonal opposite bolt on bottom frames and individual door for body earthing. Internally door shall be grounded with the main frame.
JNB.TR.13	Door Open Switch	Required for alarm extension, fan working and lighting. In case of any door open, alarm shall be generated.
JNB.TR.14	Free Space	Free Space: minimum 4U
Electrical Specifications		
Input		
JNB.TR.15	System Usable Capacity	2 KW (Redundancy N+1)
JNB.TR.16	Input Voltage Range	230 - 300 V
JNB.TR.17	Frequency (default: sync range)	50 HZ
JNB.TR.18	Protection	Inbuilt Short Circuit, Over/ Under Voltage
JNB.TR.19	Surge Protection	Class C type (IEC 61643-1 , UL 94-0)
JNB.TR.20	Power Factor / THD	> 0.9 at 50% load or more / < 5%
AC Output		
JNB.TR.21	Maximum Capacity	300 W
JNB.TR.22	Nominal System output Voltage	220V AC/ Sine Wave
JNB.TR.23	Frequency	50Hz +- 5%
JNB.TR.24	Overload Protection	Yes
JNB.TR.25	THD	<5%
JNB.TR.26	Protection	Short Circuit, Over Temperature
JNB.TR.27	Crest Factor	3
JNB.TR.28	Efficiency	89% @ full load
JNB.TR.29	Output Ports	Miscellaneous x 2 (3 Amp)

S. No.	Nature of requirement	Minimum Requirements
General		
JNB.TR.30	Controls and Monitoring	High End Embedded Controller with LCD display
JNB.TR.31	User interface	<ul style="list-style-type: none"> <li>LEDs for local visual alarming (Major, Minor, Power ON)</li> </ul>
JNB.TR.32		<ul style="list-style-type: none"> <li>Ethernet for remote or local monitoring and control via Web browser.</li> </ul>
JNB.TR.33		<ul style="list-style-type: none"> <li>SNMP V2 &amp; V.3.0 protocol with TRAP, SET and GET on Ethernet. Email of TRAP alarms</li> </ul>
JNB.TR.34	Operating temperature	0 to +65 °C
JNB.TR.35	Battery Technology	Support both VRLA/SMF and Lithium Iron Phosphate.
JNB.TR.36	Management	Monitoring battery alarms and parameters with led indications.
JNB.TR.37	Battery Backup	1 Hrs

#### 7.5.5 Junction Box 2 KVA (Outdoor Utility Cabinet)

S. No.	Nature of requirement	Minimum Requirements
JNB.TR.01	Mechanical Structure	Out Door Cabinet with Floor Mount provision
JNB.TR.02		Material - Galvanized Iron (GI) Sheet
JNB.TR.03		Thickness - Enclosure structure using 1.6 mm
JNB.TR.04		Foot plinth panel sheet minimum 3mm
JNB.TR.05	Ingress Protection	IP 55 Rated
JNB.TR.06	Colour	Colour - Grey / Relevant
JNB.TR.07	Coating thickness	Powder coating thickness between 70 to 120 micron Finish
JNB.TR.08	Cables	Cable management must be ensure proper path for AC supply
JNB.TR.09	Cable Entry	Cable entry on side bottom/Side wall through cable glands of PVC material to ensure rain water protection.
JNB.TR.10	Cooling	Forced air cooling to maintain approx. T < 10 Degree
JNB.TR.11	Filter	Removable and washable type pleated filters with aluminium wire mesh protection on both sides.
JNB.TR.12	Earthing	Diagonal opposite bolt on bottom frames and individual door for body earthing. Internally door shall be grounded with the main frame.
JNB.TR.13	Door Open Switch	Required for alarm extension, fan working and lighting. In case of any door open, alarm shall be generated.
JNB.TR.14	Free Space	Free Space: minimum 8U
Electrical Specifications		
Input		

S. No.	Nature of requirement	Minimum Requirements
JNB.TR.15	System Usable Capacity	4 KW (Redundancy N+1)
JNB.TR.16	Input Voltage Range	230 - 300 V
JNB.TR.17	Frequency (default: sync range)	50 HZ
JNB.TR.18	Protection	Inbuilt Short Circuit, Over/ Under Voltage
JNB.TR.19	Surge Protection	Class C type (IEC 61643-1 , UL 94-0)
JNB.TR.20	Power Factor / THD	> 0.9 at 50% load or more / < 5%
AC Output		
JNB.TR.21	Maximum Capacity	300 W
JNB.TR.22	Nominal System output Voltage	220V AC/ Sine Wave
JNB.TR.23	Frequency	50Hz +- 5%
JNB.TR.24	Overload Protection	Yes
JNB.TR.25	THD	<5%
JNB.TR.26	Protection	Short Circuit, Over Temperature
JNB.TR.27	Crest Factor	3
JNB.TR.28	Efficiency	89% @ full load
JNB.TR.29	Output Ports	Miscellaneous x 2 (3 Amp)
General		
JNB.TR.30	Controls and Monitoring	High End Embedded Controller with LCD display
JNB.TR.31	User interface	<ul style="list-style-type: none"> <li>LEDs for local visual alarming (Major, Minor, Power ON)</li> </ul>
JNB.TR.32		<ul style="list-style-type: none"> <li>Ethernet for remote or local monitoring and control via Web browser.</li> </ul>
JNB.TR.33		<ul style="list-style-type: none"> <li>SNMP V2 &amp; V.3.0 protocol with TRAP, SET and GET on Ethernet. Email of TRAP alarms</li> </ul>
JNB.TR.34	Operating temperature	0 to +65 °C
JNB.TR.35	Battery Technology	Support both VRLA/SMF and Lithium Iron Phosphate.
JNB.TR.36	Management	Monitoring battery alarms and parameters with led indications.
JNB.TR.37	Battery Backup	1 Hrs

## 7.6 Data Centre

### 7.6.1 Surveillance Storage (1300 TB NL SAS Drives Usable Capacity)

S. No.	Nature of Requirement	Minimum Specification
PS.TR.001	Converge/ Unified Storage	Unified Storage/Truly converge Solution with NSPoF (No single point of failure) Architecture. The Storage solution should support NAS & SAN as an integrated offering with high availability at each level. The architecture should allow upgrades of hardware and software for investment protection.
PS.TR.002	Protocols	Solution should be configured with required protocols for the solution CIFS/SMB 3/ NFS 4/iSCSI/FCoE/FC. All required protocols required for the solution to be enabled.
PS.TR.003	Controllers	System to have minimum Two controllers with NSPoF Architecture (NO single point of failure architecture). System Data mover/controller should support 2x Intel Xeon E5-2600 8- core CPU or higher. Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.
PS.TR.004	Operating System	The storage array should support Operating System Platforms & Clustering including: Linux/Windows
PS.TR.005	Cache Memory	Cache Memory: Each controller/node should be provided with minimum 128 GB RAM scalable to 512 GB RAM with usable protected data Cache for Disk IO Operations. If NAS controllers with separate controllers additional RAM cache to be provided. The storage array must have complete cache protection mechanism either by de-staging data to disk/flash or protecting with NVRAM
PS.TR.006	Host	The storage system shall be capable of providing host connectivity as per solution offered (Unified/SAN/NAS/Scale out NAS).
PS.TR.007	Connectivity	Minimum 2 ports per controller to be provided for host connectivity
PS.TR.008	RAID Supports	RAID levels Supported: 0, 1, 5, 6, 10 ( Dual parity or higher)
PS.TR.009	Redundancy	Fans and power supplies: Dual redundant, hot-swappable
PS.TR.010	Disk Drive Support	Storage subsystem shall support 4TB/6TB/8TB or higher NLSAS/SATA/equivalent 7.2K drives in the same device array.
PS.TR.011	Global Hot Spare	System should have the capability to designate global hot spares that can automatically be used to replace a failed drive anywhere in the system. Storage system should be configured with required Global Hot-spares for the different type and no. of

S. No.	Nature of Requirement	Minimum Specification
		disks configured, as per the system architecture best practices.
PS.TR.012	Capacity	The storage system to be configured with 45 TB SSD & 60 TB of NL-SAS drives capacity for application storage.
PS.TR.013	Thin Provisioning	Proposed array must be supplied with Thin provisioning for the configured capacity.
PS.TR.014	De-duplication	Should provide de-duplication functionalities for the configured capacity.
PS.TR.015	Tiering	Storage should support inbuilt automated tiering feature that migrates the most frequently accessed data to the SSD/RAM. Necessary licenses for configured capacity to be provided from day 1
PS.TR.016	Snapshots	Should be able to take "snapshots" of the stored data. Offered Storage shall have support to make the snapshot in scheduled or auto snaps. Snapshot should support both block and file.
PS.TR.017	Replication	The storage array must have the capability to do remote replication using IP technology.
PS.TR.018	Software Licenses	All the necessary software and licenses to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots, compression, de-dup, replication, auto-tiering for the configured capacity to be provided from day 1
PS.TR.019	Monitoring	Should support the functionality of monitoring of Disk drive and Storage system for all possible hard or soft failure.

#### 7.6.2 SAN Switch

S. No.	Nature of Requirement	Minimum Specification
SAN.TR.001	Converge/ Unified Storage	The fibre switch should be quoted with minimum 48 FC ports of 16Gbps speed with all supported Licenses from day one.
SAN.TR.002	Protocols	The switch should have support for 8/16 Gbps HBA
SAN.TR.003	Controllers	The switch should have auto sensing, Zoning, Integrated Ethernet and Serial Port for communication.
SAN.TR.004	Operating System	Switch should be rack mountable 1U size and should be supplied with mounting kit.
SAN.TR.005	Cache Memory	The switch should be equipped with redundant hot swap power supply and Fan and allow hot swap ability without resetting the switch, or affecting the operations of the switch
SAN.TR.006	Host	The switch should be backward compatible
SAN.TR.007	Connectivity	The switch should be capable for Non-disruptive firmware /microcode upgrade and hot code activation.

S. No.	Nature of Requirement	Minimum Specification
SAN.TR.008	RAID Supports	The switch should be capable of End to end performance monitoring
SAN.TR.009	Redundancy	The switch should have Support for POST & online /offline diagnostics , non-disruptive daemon restart FC ping and path info(FC trace route)
SAN.TR.010	Disk Drive Support	The switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems
SAN.TR.011	Global Hot Spare	The switch should have following Zoning and security features -
SAN.TR.012	Capacity	a. Support for hardware and software zoning and ACL
SAN.TR.013	Thin Provisioning	b. Policy based security and centralized fabric management.
SAN.TR.014	De-duplication	c. Support for secure access.
SAN.TR.015	Tiering	d. Support for FC based authentication.
SAN.TR.016	Snapshots	e. Support for RADIUS, SSH, SNMP
SAN.TR.017	Replication	f. Support for port binding.
SAN.TR.018	Software Licenses	g. Support for port masking.
SAN.TR.019	Monitoring	h. Support for Hardware based Inter Switch linking / trunking.
SAN.TR.020		i. Support for dynamic Load balancing of links with no overhead.
SAN.TR.021		Support for web based management and should also support CLI. Switch shall support alert based on threshold value for temperature, fan status, power supply status and port status.
SAN.TR.022		The switch shall support different port type such as FL port, F port ,M port(mirror port), and E port ; self-discovery based on switch type ( U port ); optional port type control in access gateway mode F port and NPIV-Enabled N port.
SAN.TR.023		All relevant licenses for all the above features and scale should be quoted along with switch

### 7.6.3 Unified storage with SAN Switch (125TB for Video and Application Data)

S. No.	Minimum Requirement Description
SNS.TR.01	The fiber switch should be quoted with minimum 48 FC ports of 16Gbps speed each with all supported Licenses from day one.
SNS.TR.02	The switch should have support for 8/16 Gbps HBA
SNS.TR.03	The switch should have auto sensing, Zoning, Integrated Ethernet and Serial Port for communication.
SNS.TR.04	Switch should be rack mountable 1U size and should be supplied with mounting kit.
SNS.TR.05	The switch should be equipped with redundant hot swap power supply and Fan and allow hot swap ability without resetting the switch, or affecting the operations of the switch

S. No.	Minimum Requirement Description
SNS.TR.06	The switch should be backward compatible
SNS.TR.07	The switch should be capable for Non-disruptive firmware /microcode upgrade and hot code activation.
SNS.TR.08	The switch should be capable of End to end performance monitoring
SNS.TR.09	The switch should have Support for POST & online /offline diagnostics , non-disruptive daemon restart FC ping and path info(FC trace route)
SNS.TR.10	The switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple Operating Systems
SNS.TR.11	The switch should have following Zoning and security features -
SNS.TR.12	a. Support for hardware and software zoning and ACL
SNS.TR.13	b. Policy based security and centralized fabric management.
SNS.TR.14	c. Support for secure access.
SNS.TR.15	d. Support for FC based authentication.
SNS.TR.16	e. Support for RADIUS, SSH, SNMP
SNS.TR.17	f. Support for port binding.
SNS.TR.18	g. Support for port masking.
SNS.TR.19	h. Support for Hardware based Inter Switch linking / trunking.
SNS.TR.20	i. Support for dynamic Load balancing of links with no overhead.
SNS.TR.21	Support for web based management and should also support CLI. Switch shall support alert based on threshold value for temperature, fan status, power supply status and port status.
SNS.TR.22	The switch shall support different port type such as FL port, F port ,M port(mirror port), and E port ; self-discovery based on switch type ( U port ); optional port type control in access gateway mode F port and NPIV-Enabled N port.
SNS.TR.23	All relevant licenses for all the above features and scale should be quoted along with switch

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

S. No.	Nature of Requirement	Specification
BLD.TR. 01	CPU	Each blade shall have two numbers of latest Intel Xeon Scalable Processors (Intel® Xeon® 6000 processor family or higher) with Min. 18 cores per processor each having Min. 2.3 GHz processor speed.
BLD.TR. 02	Motherboard	Intel chipset compatible with the offered processors.
BLD.TR. 03	Memory	Min. 24 DIMM slots, should be provided with 256 GB RAM using DDR4 DIMM's operating at 2666 MT/s (depending on processor model)
BLD.TR. 04	Memory Protection	Advanced ECC with multi-bit error protection, online mirror memory
BLD.TR. 05	Hard disk drive with carrier	2*400 GB 3X DWPD SSD drives
BLD.TR. 06	Storage Controller	SAS Raid Controller with RAID 0/1

S. No.	Nature of Requirement	Specification
BLD.TR.07	Networking features	The server should provide a minimum of 40 Gbps of bandwidth with Converged network adapter ports across two or more cards.
BLD.TR.08	Interfaces	Minimum of 1* internal USB 3.0 port ,1* internal SD card slot
BLD.TR.09	Bus Slots	Minimum of 2 Nos of PCIe 3.0 based mezzanine slots supporting Converged Ethernet adapters
BLD.TR.10	Redundancy	The blades to be provided with port level & card level redundancy
BLD.TR.11	Operating System and Virtualization Support	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), VMware, SUSE Linux Enterprise Server (SLES)
BLD.TR.12	Warranty	5 year OEM Warranty

#### 7.6.5 Rack - 42 U with necessary cabling

S. No.	Minimum Requirement Description
RK.TR.01	42U (600x1000)
RK.TR.02	Aluminium
RK.TR.03	Provision for heat dissipation for side-to-side and Front-to-Back units
RK.TR.04	Top and Bottom gland cable Entry trays with brush
RK.TR.05	Full Side Panels for both sides
RK.TR.06	Front door with latch and ventilation holes.
RK.TR.07	Back door with latch and ventilation holes.
RK.TR.08	2* Dual 32 A PDU
RK.TR.09	2* 16 receptacle Power Connectors each connected to separate PDUs
RK.TR.10	Keyboard Drawer, 2x fixed tray
RK.TR.11	Nuts and washers for mounting equipment and slides.
RK.TR.12	Adequate cable manager for units
RK.TR.13	4 * Depth Support channels

#### 7.6.6 Blade Chassis with Switch and virtual KVM

S. No.	Nature of Requirement	Specification
BLC.TR.01	Enclosure	OEM of the proposed solution should be listed in Leaders/Challengers Quadrant of Gartner's latest report for modular servers  Blade chassis shall be 19" Electronic Industries Alliance Standard Width rack mountable and provide appropriate rack mount kit  The enclosure Should support full height/width and half height/width blades in the same enclosure, occupying a max of 10U rack height, it should support minimum 8 blade servers

S. No.	Nature of Requirement	Specification
	Power	The enclosure should be populated fully with power supplies of the highest capacity & energy efficiency of platinum rating.
		The power subsystem should support N + N, N+1 power redundancy (where N is greater than 1) for a fully populated chassis with all servers configured with the highest CPU configuration ( 150 W and above),
BLC.TR.02	Blade Support	Each blade enclosure should have a cooling subsystem consisting of redundant hot pluggable fans or blowers enabled with technologies for improved power consumption and acoustics
		Enclosure should support all Intel Xeon Scalable processors based 2 CPU and 4 CPU blades
		Should support built-in management software in redundancy
BLC.TR.03	Converged Module	Should provide single management console for all the blade servers across multiple chassis.
		The chassis should be provided with redundant modules for connectivity
		Chassis should have sufficient number of redundant 40gb based converged modules to provide a minimum FCOE uplink bandwidth of 20Gbps per blade server and 10Gbps sustained per blade server ( with 1 module failure)for a fully populated chassis for converged Traffic.
BLC.TR.04	Chassis Management software	Chassis should support aggregation of multiple enclosures to consolidate data centre network connections, reduce hardware and to scale network bandwidth across multiple enclosures (minimum 4 enclosures). All the modules/switches for chassis interconnectivity should be in redundancy.
		The chassis aggregation switch should provide a Minimum of 6*10 Gb Ethernet & 6*16 GB FC uplinks per switch should be provided for external connectivity

S. No.	Nature of Requirement	Specification
		the features to be supplied for fully populated chassis.
		Centralized Redundant Management solution should be provided so that management of all blade servers across multiple chassis within Data Centre can be done from single console If required the management of rack servers should be possible from same console. If the management system runs as a virtual machine , then all hardware and software licenses to enable this should be included
		Should support auto-discovery of resources within an enclosure and on multiple connected enclosures.
		Solution should support templates to quickly make changes to the infrastructure. the server BIOS version, MAC ID, NIC firmware version, WWPN , FC-HBA firmware version , Adapter QoS , Management module firmware version, UUIDs , Server Boot Policies, KVM IP etc. of the infrastructure required for workload
		The management software should be used to create resource pools and have the blade resources assigned to the respective resource pools & re-assign resources to effectively utilize infrastructure
		Role Based Access Control with at least 6 users to define roles and privileges and remote management capabilities including remote KVM should be included
BLC.TR.05	Warranty	5 year OEM Warranty

#### 7.6.7 Internet Router

S. No.	Nature of Requirement	Minimum Requirement Description
IR.TR.01	Architecture	The router shall facilitate all applications like voice, video and data to run over a converged IP infrastructure along with hardware assisted IPSEC & Network Address Translation (NAT), capability. The router shall also support hitless interface protection, In-band and out-band management, Software rollback feature, Graceful Restart, non-stop routing for OSPF, BGP, LDP, MP-BGP etc. The platform shall have modular software that shall run service &

S. No.	Nature of Requirement	Minimum Requirement Description
		features as processes having full isolation from each other.
IR.TR.02		The router shall support following interface: Gigabit Ethernet, Channelized STM1, STM1, STM16, STM64, 10G Ethernet, POS, V.35 Serial Ports, E1, Chn E1, E3 Ports.
IR.TR.03		<p>Backplane Architecture: The back plane architecture of the router must be modular and redundant.</p> <p>The routing aggregate throughput should be at least 5 Gbps which can scale up to 20 Gbps to meet future requirement without changing the hardware.</p> <p>Should support minimum 8Mpps and scalable up to 15 Mpps of forwarding performance</p>
IR.TR.04	Performance	<ul style="list-style-type: none"> <li>-The Router should have individual dedicated control plane processor and data plane processor module. Data plane Processor module should be independent of the control plane Processor. Control plane Processor should have support for internal memory to support multiple software images for backup purposes and future scalability.</li> <li>-The router processor architecture must be multi-processor based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.</li> <li>-The proposed router shall support 2M NAT 44 sessions and 2M NAT64 Stateful sessions</li> <li>-The proposed router shall support minimum 2000 VRFs</li> </ul>
IR.TR.05		<ul style="list-style-type: none"> <li>-The router shall support the IPv4 and IPv6 DUAL-stack in hardware and software.</li> <li>-The router shall support minimum 1M IPv4 &amp; IPv6 routes from day one (1) &amp; scalable to minimum 3MN IPv4 &amp; IPv6 unicast routes in FIB in future</li> <li>-Shall have 18 K Multicast routes &amp; 1000 IGMP groups.</li> </ul>
IR.TR.06	Protocol Support	The router shall have RIPv1, RIPv2, RIPng, BGP, OSPFv2 & v3, Policy Based Routing for both IPv4 & IPv6, IP Multicast Routing Protocols to facilitate applications such as streaming, webcast, command & control including PIM SM, PIM SSM, GRE (Generic Routing Encapsulation).

S. No.	Nature of Requirement	Minimum Requirement Description
IR.TR.07		The router should have support for 4,000 IPSEC tunnels and 1000 tunnels of GRE.
IR.TR.08		Router shall support following MPLS features – LDP, Layer 2 VPN such as EoMPLS or equivalent with LDP signaling, Route Reflector (RR), Traffic Engineering with RSVP-TE, Fast Reroute Link Node & Path protection enabled.
IR.TR.09	QoS Features	The router shall support QoS policy in the router shall support dual Strict Priority Queue or Low Latency Queue per policy so that voice and video traffic can be put in different queue. It also should have hierarchical QOS (Inbound and Outbound) to ensure bandwidth allocation for all type of traffic during congestion and non-congestion scenario.
IR.TR.10		The router shall perform traffic Classification using various parameters like source physical interfaces, source/destination IP subnet, protocol types (IP/TCP/UDP), source/destination ports, IP Precedence, 802.1p, DSCP and by some well-known application types through Application Recognition techniques.
IR.TR.11	Security Feature	The router shall support for hardware enabled Network Address Translation (NAT) and Port Address Translation (PAT). The router shall support NAT6to4 function & vrf-aware NAT function.
IR.TR.12		The router shall meet the following requirements for security: Access Control List to filter traffic based on Source & Destination IP Subnet, Source & Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc) and Port Range etc. Router shall support deep and Stateful packet inspection to recognize a wide variety of applications
IR.TR.13		The router shall support firewall service with Stateful firewall & zone based firewall protection. The firewall performance shall be at least 2 Gbps (Internal/External). In case of external firewall, bidder shall propose the firewall with necessary interfaces.
IR.TR.14		Router shall support IPsec (Internal/external) with at least 2 Gbps of IPSEC throughput and VRF aware IPsec. If it is external box then hardware should be provided along with the router.
IR.TR.16	Management	The router shall support management through SNMPv1/v2/v3, support RADIUS and TACACS.

S. No.	Nature of Requirement	Minimum Requirement Description
		The router shall role based access to the system for configuration and monitoring & deep and Stateful packet inspection to recognize a wide variety of applications. The router shall be provided with IETF standards based feature so that granular traffic analysis can be performed for advanced auditing, usage analysis, capacity planning or generating security telemetry events, also the router shall have SLA monitoring tools to measure state of the network in real time. The SLA Operations shall provide information on TCP/UDP delay, jitter, application response time, Packet Loss etc.
IR.TR.17	Interface Requirements:	Router shall be provided with 6 x 1 GE port with 2xSM & 4x1G copper transceivers & two 10G SR based Port
IR.TR.18	Compliance/ Certifications	The proposed router shall be IPv6 Phase 2 certified by accredited lab of IPv6 Ready forum.
IR.TR.19	Compliance/ Certifications	The Router shall be minimum EAL2 / Applicable Protection Profile (NDPP) certified under the Common Criteria Evaluation Program.

#### 7.6.8 Core Router

S. No.	Nature of Requirement	Minimum Requirement Description
CR.TR.01	Architecture	Router should have redundant controller cards (redundant control & data plane) and should support Stateful switchover, non-stop forwarding, Non-stop routing and Graceful restart.
CR.TR.02		Router should be CE2.0/MEF14.0 certified
		Router shall support MEF for Ethernet based services like PW, VPLS or ATOM.
		Router shall support sync any configurations from previous modules to new modules with hot-swap event occurred
		The router shall support following type of interfaces – 10GE, 1GE interfaces and 10G.
		All the Ports and card on Router should be hot swappable and field replacement of port or card should not bring down the chassis.
CR.TR.03	Performance	Router shall support minimum non-blocking capacity of 40 Gbps with scalability of up to 60Gbps without changing the hardware
		Router shall support 60 Mpps forwarding performance for IPv4 & IPv6 performance
		Router shall support 16000 Mac addresses
		Router shall support 18000 IPv4 routes

S. No.	Nature of Requirement	Minimum Requirement Description
		<p>router shall support 4000 queues and 128 MPLS VPN's</p> <p>Router shall support aggregation of links. Minimum 8 links should be supported as part of single aggregation</p> <p>Router shall support IPSLA or equivalent and Y.1731 for performance monitoring</p>
CR.TR.04	High Availability	<p>Router should support Redundant Power Supply and should also support Online insertion and removal of same.</p> <p>Fan tray should be hot-swappable and should be a Field Replaceable Unit (FRU). The node can run indefinitely with a single fan failure. Shall Support hot-swappable for all modules. And secure normal operations when hot-swap event occurred</p> <p>Router shall support MPLS-TE with FRR for sub 50 msec protection.</p> <p>Router must support Traffic Engineering for node and link protection.</p>
CR.TR.05	Protocol Support	<p>Router shall support IPV4 and IPV6, IGMP V2/V3, MLD, IGMP and PIM, 6PE and 6VPE</p> <p>mode for IPV6 transport over IPV4, ECMP, LDP, BGP Prefix independent control (EDGE and Core) for IPV4 and IPV6, BGP, ISIS, OSPFv2 and V3, RSVP, VRRP and Traffic Engineering</p> <p>Router should support high availability for all BFD, BGP, OSPF and IS-IS and no packet loss during controller switch over.</p> <p>Router should support RFC 3107 of Carrying Label Information in BGP-4</p> <p>The Router should support Point to Point and Point to Multipoint LSP for Unicast and Multicast traffic.</p> <p>Router shall support layer3 and layer2 MPLS VPN.</p>
CR.TR.06	QoS Features	<p>Router shall support HQOS on all kind of interface in both ingress and egress direction. Similar QOS shall be supported for all type of interface including Bundled interfaces.</p> <p>Shall support Ingress classification, marking and policing on physical interfaces and logical interfaces using source/destination IP subnet, protocol types (IP/TCP/UDP),source/destination ports, IP Precedence, MPLS EXP, DSCP,802.1p</p> <p>Shall support Strict Priority Queuing or Low Latency Queuing to support real-time</p>

S. No.	Nature of Requirement	Minimum Requirement Description
		application like Voice and Video with minimum delay and jitter.
		Congestion Management: WRED, Priority queuing, Class-based weighted fair queuing
CR.TR.07	Security & Management	Support Access Control List to filter traffic based on Source & Destination IP Subnet, Source& Destination Port, Protocol Type (IP, UDP, TCP, ICMP etc.) and Port Range etc. Should Support per-user Authentication, Authorization, and Accounting through RADIUS or TACACS and SNMPv1/v2/V3
CR.TR.08	Operating Environmental Requirements	0°C to 40°C operating temperature and 10 to 90%, non-condensing
CR.TR.09	Interface	The proposed router should be provided with the following interfaces from day1: - 4x10G with 2 x multimode transceiver 4x1G SFP port with 2x1G single mode transceiver 4x 10/100/1000base-T Ethernet Ports.
CR.TR.10	Certifications/ OEM Criteria	The proposed router should be EAL2/ NDPP certified by common Criteria body at the time of delivery.

#### 7.6.9 Spine Switch

S. No.	Minimum Requirement Description
	General Requirement
SS.TR.01	The core/spine layer switches should have hardware level redundancy (1+1) in terms of data plane and control plane. Issues with any of the plane should not impact the functioning of the switch.
SS.TR.02	The switch should have redundant CPUs working in active-active or active-standby mode. CPU fail over/change over should not disrupt/impact/degrade the functioning the switch.
SS.TR.03	The Switch should support non-blocking Layer 2 switching and Layer 3 routing. Switch with different modules should function line rate and should not have any port with oversubscription ratio applied
SS.TR.04	Switch should support in line hot insertion and removal of different parts like modules/power supplies/fan tray etc. This should not require rebooting of the switch or create disruption in the working/functionality of the switch
SS.TR.05	Switch should support the complete STACK of IP V4 and IP V6 services.
SS.TR.06	Switch and optics must be from the same OEM
SS.TR.07	Switch should support non-blocking, wire speed performance per line card
SS.TR.08	OEM should be rated as a leader/challengers in latest Gartner Magic Quadrant report for DC Switching
	Hardware and Interface Requirement

S. No.	Minimum Requirement Description
SS.TR.09	Switch should have the following interfaces:
SS.TR.10	a. Minimum 32 nos. of line rate and Non - Blocking 40/100G ports populated with 8x40G Bidi transceivers from day one
SS.TR.11	Switch should have adequate power supplies for the complete system usage , providing N+1 redundancy
SS.TR.12	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/Link Aggregation Group (LAG) etc
SS.TR.13	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
	Performance Requirement
SS.TR.14	The switch should support 1 million IPv4 routes or above
SS.TR.15	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG
SS.TR.16	Switch should support minimum 1000 VRF instances
SS.TR.17	Switch should support total aggregate minimum 28 Tbps minimum of switching capacity considering future scalability
	Virtualization Features
SS.TR.18	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)/NVGRE as per RFC 2890
SS.TR.19	Switch should support VXLAN (RFC7348) and EVPN control plane
SS.TR.20	Switch should support Open Flow/Open Day light/Open Stack controller
SS.TR.21	Switch should support multi OEM hypervisor environment and should be able to sense movement of VM and configure network automatically
SS.TR.22	Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation
	Layer2 Features
SS.TR.23	Switch should support minimum 92,000 no. of MAC addresses
SS.TR.24	Switch should support Jumbo Frames up to 9K Bytes on 40G/100G Ports
SS.TR.25	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
	Layer3 Features
SS.TR.26	Switch should support Policy based and segment routing
SS.TR.27	Switch should provide multicast traffic reachable using:
SS.TR.28	a. PIM-SM
SS.TR.29	b. PIM-SSM
SS.TR.30	c. Bi-Directional PIM
SS.TR.31	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
SS.TR.32	e. IGMP V.1, V.2 and V.3
SS.TR.33	Switch should support Multicast routing
	Availability
SS.TR.34	Switch should support for BFD For Fast Failure Detection
	Quality of Service
SS.TR.35	Switch should have a minimum buffer of 80 Mb
	Security
SS.TR.36	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined

S. No.	Minimum Requirement Description
SS.TR.37	Switch should support for external database for AAA using:
SS.TR.38	a. TACACS+
SS.TR.39	b. RADIUS
SS.TR.40	Should support Standard & Extended ACLs
SS.TR.41	Switch should support MAC ACLs
	Manageability
SS.TR.42	Switch should support for predefined and customized execution of script for device mange for automatic and scheduled system status update for monitoring and management
SS.TR.43	Switch should provide different privilege for login in to the system for monitoring and management
SS.TR.44	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
SS.TR.45	All relevant licenses for all the above features and scale should be quoted along with switch

#### 7.6.10 Leaf (TOR) Switch

S.No.	Minimum Requirement Specification
	Solution Requirement
LS.TR.01	The Switch should support non-blocking Layer 2 switching and Layer 3 routing
LS.TR.02	There switch should not have any single point of failure like power supplies and fans etc should have 1:1/N+1 level of redundancy
LS.TR.03	Switch and optics must be from the same OEM
LS.TR.04	Switch should support the complete STACK of IP V4 and IP V6 services.
	Hardware and Interface Requirement
LS.TR.05	Switch should have the following interfaces:
LS.TR.06	a. 48 x 10G/25G Interface with 32x10G SR & 8x1G Transceiver
LS.TR.07	b. 6 x 40/100GbE QSFP ports populated with 2x40G bidi transceiver for Spine connectivity; it should also support native 256 ports
LS.TR.08	Switch should support for different logical interface types like loopback, VLAN, SVI, Port Channel, multi chassis port channel/LAG etc
LS.TR.09	Switch should support IEEE Link Aggregation and Ethernet Bonding functionality to group multiple ports for redundancy
	Performance Requirement
LS.TR.10	The switch should support 12,000 IPv4 and IPv6 routes entries in the routing table including multicast routes
LS.TR.11	The switch should support hardware based load balancing at wire speed using LACP and multi chassis ether channel/LAG
LS.TR.12	Switch should support minimum 3.6 Tbps of switching capacity
LS.TR.13	Switch should support minimum 1000 VRF instances
LS.TR.14	Each leaf should have connectivity to all spine switches over 40Gbps minimum
	Advance Features
LS.TR.15	Switch should support Network Virtualization using Virtual Over Lay Network using VXLAN (RFC 7348)

S.No.	Minimum Requirement Specification
LS.TR.16	Switch should support VXLAN (RFC7348) and EVPN or equivalent for supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the data center
LS.TR.17	Switch must support VXLAN Switching/Bridging and VXLAN Routing without any performance degradation
	Layer2 Features
LS.TR.18	Switch should support minimum 92,000 no. of MAC addresses
LS.TR.19	Switch should support Jumbo Frames up to 9K Bytes on all Ports
	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities
	Layer3 Features
LS.TR.20	Switch should support Policy based & segment routing
LS.TR.21	Switch should provide multicast traffic reachable using:
LS.TR.22	a. PIM-SM
LS.TR.23	b. PIM-SSM
LS.TR.24	c. Bi-Directional PIM
LS.TR.25	d. Support RFC 3618 Multicast Source Discovery Protocol (MSDP)
LS.TR.26	e. IGMP V.1, V.2 and V.3
LS.TR.27	Switch should support Multicast routing
LS.TR.28	Switch should support for BFD For Fast Failure Detection
	Quality of Service
LS.TR.29	Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x and should have a minimum buffer of 40 Mb
	Security
LS.TR.30	Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy
LS.TR.32	Switch should support for external database for AAA using:
LS.TR.33	a. TACACS+
LS.TR.34	b. RADIUS
LS.TR.35	Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined
LS.TR.36	Should support Standard & Extended ACLs; it should also support MAC ACLs
	Manageability
LS.TR.37	Switch should support for predefined and customized execution of script for device management for automatic and scheduled system status update for monitoring and management
LS.TR.38	Switch should support Real time Packet Capture using Wireshark in real time for traffic analysis and fault finding
LS.TR.39	OEM should be rated as a leader/challenger in latest Gartner Magic Quadrant report for DC Switching
LS.TR.40	All relevant licenses for all the above features and scale should be quoted along with switch

### 7.6.11 Internet Firewall

S. No.	Minimum Requirement Description
	Industry Certifications and Evaluations
IF.TR.001	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years
	Hardware Architecture
IF.TR.002	The appliance based security platform should provide firewall, AVC, AMP and IPS functionality in a single appliance from day one
IF.TR.003	The appliance should have atleast 8x1G Copper ports & 4 x10G ports with multi-mode transceiver from day one and should be scalable to additional 6 * 10G in future
IF.TR.004	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory
IF.TR.005	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.
	Performance & Scalability
IF.TR.006	Should support 4 Gbps of NGFW / Threat Prevention (FW, AVC & IPS) real-world / production performance
IF.TR.007	Firewall should support atleast 18,00,000 concurrent sessions with application visibility turned on
IF.TR.008	Firewall should support atleast 25,000 connections per second with application visibility turned on
IF.TR.009	Firewall should support Active-Standby, Active-Active high availability deployment modes. When deployed in Active-Active it should increase the overall throughput along with increase in number of connections and connections per second
IF.TR.010	Firewall should have integrated redundant hot-swappable power supply
IF.TR.011	Firewall should have integrated redundant hot-swappable fan trays/ Modules
IF.TR.012	Firewall should not consume more than 1 RU of rack space
	Firewall Features
IF.TR.013	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc
IF.TR.014	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
IF.TR.015	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
IF.TR.016	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
IF.TR.017	Should support Multicast protocols like IGMP, PIM, etc
IF.TR.018	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
IF.TR.019	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.

S. No.	Minimum Requirement Description
IF.TR.020	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.
IF.TR.021	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness
IF.TR.022	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
IF.TR.023	Should support more than 25,000 (excluding custom signatures) IPS signatures or more
IF.TR.024	Should be capable of supporting at least 60-70 number of URL filtering categories with 200M URL categorized
IF.TR.025	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
IF.TR.026	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
IF.TR.027	Should be capable of detecting and blocking IPv6 attacks.
IF.TR.028	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
IF.TR.029	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
IF.TR.030	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
IF.TR.031	Solution should support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
IF.TR.032	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on premise on purpose built-appliance
IF.TR.033	Solution shall have capability to analyse and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP
IF.TR.034	Proposed solution shall have required subscription like Threat Intelligence for proper functioning
IF.TR.035	Local Malware analysis/sandboxing appliance shall be capable of executing MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries or more in a virtual environment.
IF.TR.036	Local Malware analysis/sandboxing appliance shall have integrated redundant power supply and minimum of 2 x 10 Gig ports or more

S. No.	Minimum Requirement Description
IF.TR.037	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
IF.TR.038	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
IF.TR.039	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location
IF.TR.040	The detection engine should support the capability of detecting variants of known threats, as well as new threats
IF.TR.041	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. I
IF.TR.042	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
	Management
IF.TR.0043	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
IF.TR.044	The management platform must be a dedicated OEM appliance and VM running on server shall not be accepted
IF.TR.045	The management appliance should have 2 x 1G port and integrated redundant power supply from day one
IF.TR.046	The management platform must be able to store record of 15000 user or more
IF.TR.047	The management platform must provide a highly customizable dashboard.
IF.TR.048	The management platform must domain multi-domain management
IF.TR.049	The management platform must provide centralized logging and reporting functionality
IF.TR.050	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
IF.TR.051	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
IF.TR.052	Should support troubleshooting techniques like Packet tracer and capture
IF.TR.053	Should support REST API for monitoring and config programmability
IF.TR.054	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
IF.TR.055	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
IF.TR.056	The centralized management platform must not have any limit in terms of handling logs per day

S. No.	Minimum Requirement Description
IF.TR.057	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
IF.TR.058	The management platform support running on-demand and scheduled reports
IF.TR.059	The management platform must risk reports like advanced malware, attacks and network
IF.TR.060	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

### 7.6.12 Internal Firewall

S. No.	Minimum Requirement Description
Industry Certifications and Evaluations	
ITF.TR.01	The Firewall solution offered must be rated as 'leaders' or 'Challengers' in the latest Magic Quadrant for Enterprise Firewall published by Gartner from last 3 years
Hardware Architecture	
ITF.TR.02	The appliance based security platform should provide firewall, AVC and IPS functionality in a single appliance from day one
ITF.TR.03	The appliance should support atleast 6x1G Ethernet Ports & 4 x 10G ports with multi-mode transceiver from day one and should be scalable to additional 6 x10G in future
ITF.TR.04	The appliance hardware should be a multicore CPU architecture with a hardened 64 bit operating system to support higher memory
ITF.TR.05	Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.
Performance & Scalability	
ITF.TR.06	Should support 6 Gbps of NGFW / Threat Prevention (FW, AVC and IPS) real-world / production performance
ITF.TR.07	Firewall should support atleast 25,00,000 concurrent sessions with application visibility turned on
ITF.TR.08	Firewall should support atleast 35,000 connections per second with application visibility turned on
ITF.TR.09	Firewall should support Active-Standby, Active-Active/Clustering high availability deployment modes. When deployed in Active-Active/Clustering it should increase the overall throughput along with increase in number of connections and connections per second
ITF.TR.10	Firewall should have integrated redundant hot-swappable power supply
ITF.TR.11	Firewall should have integrated redundant hot-swappable fan tray / modules
ITF.TR.12	Firewall should not consume more than 1 RU of rack space
Firewall Features	
ITF.TR.13	Firewall should support creating access-rules with IPv4 & IPv6 objects, user/groups, application, geolocation, url, zones, vlan, etc

S. No.	Minimum Requirement Description
ITF.TR.14	Firewall should support manual NAT and Auto-NAT, static nat, dynamic nat, dynamic pat
ITF.TR.15	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality
ITF.TR.16	Should support Static, RIP, OSPF, OSPFv3 and BGP, BGPv6
ITF.TR.17	Should support Multicast protocols like IGMP, PIM, etc
ITF.TR.18	Should support capability to integrate with other security solutions to receive contextual information like security group tags/names
ITF.TR.19	Should have the capability of passively gathering information about virtual machine traffic, network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.
ITF.TR.20	Solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.
ITF.TR.21	Should support more than 3000 (excluding custom application signatures) distinct application signature as application detection mechanism to optimize security effectiveness
ITF.TR.22	Should be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
ITF.TR.23	Should support more than 25,000 (excluding custom signatures) IPS signatures or more
ITF.TR.24	Should be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
ITF.TR.25	Should be able to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.
ITF.TR.26	Should be capable of detecting and blocking IPv6 attacks.
ITF.TR.27	Should support the capability to quarantine end point by integrating with other security solution like Network Admission Control
ITF.TR.28	Solution should support full-featured NBA capability to detect threats emerging from inside the network. This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.
ITF.TR.29	The solution must provide IP reputation feed that comprised of several regularly updated collections of poor reputation of IP addresses determined by the proposed security vendor
ITF.TR.30	Solution should support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist
ITF.TR.31	The Appliance OEM must have its own threat intelligence analysis center and should use the global footprint of security deployments for more comprehensive network protection.
ITF.TR.32	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, etc.).
ITF.TR.33	Should be able to identify attacks based on Geo-location and define policy to block on the basis of Geo-location

S. No.	Minimum Requirement Description
ITF.TR.34	The detection engine should support the capability of detecting variants of known threats, as well as new threats
ITF.TR.35	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioural anomaly detection techniques. I
ITF.TR.36	Should support Open based Application ID for access to community resources and ability to easily customize security to address new and specific threats and applications quickly
ITF.TR.37	Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature (update to be provided in 300 seconds) as they transit the network and capability to do dynamic analysis on premise on purpose built-appliance
ITF.TR.38	Solution shall have capability to analyze and block TCP/UDP protocol to identify attacks and malware communications. At minimum, the following protocols are supported for real-time inspection, blocking and control of download files: HTTP, SMTP, POP3, IMAP, NetBIOS-SSN and FTP
ITF.TR.39	Proposed solution shall have required subscription like Threat Intelligence for proper functioning
	Management
ITF.TR.40	The management platform must be accessible via a web-based interface and ideally with no need for additional client software
ITF.TR.41	The management platform must be a dedicated OEM appliance and VM running on server shall not be accepted
ITF.TR.42	The management appliance should have 2 x 1G port and integrated redundant power supply from day one
ITF.TR.43	The management platform must be able to store record of 15000 user or more
ITF.TR.44	The management platform must provide a highly customizable dashboard.
ITF.TR.45	The management platform must domain multi-domain management
ITF.TR.46	The management platform must provide centralized logging and reporting functionality
ITF.TR.47	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows
ITF.TR.48	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.
ITF.TR.49	Should support troubleshooting techniques like Packet tracer and capture
ITF.TR.50	Should support REST API for monitoring and configuration programmability
ITF.TR.51	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
ITF.TR.52	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
ITF.TR.53	The centralized management platform must not have any limit in terms of handling logs per day

S. No.	Minimum Requirement Description
ITF.TR.54	The management platform must provide built-in robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
ITF.TR.55	The management platform support running on-demand and scheduled reports
ITF.TR.56	The management platform must risk reports like advanced malware, attacks and network
ITF.TR.57	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security management applications, such as Security Information and Event Managers (SIEMs), and log management tools.

#### 7.6.13 Web Security Appliance

S. No.	Minimum Requirement Description
WSA.TR.01	Proposed solution should be in Leader / Challenger quadrant of Gartner's Web Security Gateway Magic Quadrant from last 3 years
WSA.TR.02	The solution should be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance. All the functionalities should be in a single appliance only.
WSA.TR.03	The appliance based Solution should be provided with hardened Operating System.
WSA.TR.04	The underlying operating system and hardware should be capable of supporting with 1000 users with licenses and MSI should include 200 user license from day one
WSA.TR.05	The operating system should be secure from vulnerabilities and hardened for web proxy and caching functionality.
WSA.TR.06	The solution should allow to deploy the appliance in explicit proxy as well as transparent mode together.
WSA.TR.07	The solution should support proxy configuration in a Chain. The Lower end proxies at spoke locations should be able to forward the request to an Higher end proxies at Hub Location forming a Chain of Proxies
WSA.TR.08	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains e.g. (root dns for all external domains and internal DNS for organization domain
WSA.TR.09	The solution should have facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance. This is useful in scenarios where policies are based on original IP and logging/reporting is required to track activity of individual IP basis.
WSA.TR.10	Should support active/active High Availability mode
WSA.TR.11	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy.
WSA.TR.12	The solution should support HTTPS decryption
WSA.TR.13	The solution should support scanning of the https decrypted traffic by the on-board anti-malware and/or anti-virus engines.

S. No.	Minimum Requirement Description
WSA.TR.14	The solution should provide the flexibility of deciding whether to decrypt https traffic or not to the solution administrator. The solution should offer three aspects to decide. These are:
WSA.TR.15	1) URL category based decryption
WSA.TR.16	2) Web Reputation based decryption
WSA.TR.17	3) Default action for the specific policy
WSA.TR.18	HTTPS decryption should provide flexibility to have multiple decryption policies and should not be just a Global action
WSA.TR.19	Should support the functionality to block applications that attempts to tunnel non-HTTP traffic on ports typically used for HTTP traffic.
WSA.TR.20	Should support the functionality for blocking non-SSL traffic on SSL ports & should also support the functionality to tunnel the transaction.
WSA.TR.21	The solution should act as an FTP proxy and enable organizations to exercise
WSA.TR.22	granular control, including: allow/block FTP connections,
WSA.TR.23	Restrict users/groups, control uploads/downloads, and
WSA.TR.24	Restrict sent/received files to certain types or sizes.
WSA.TR.25	The solution should be capable of blocking specific files downloads and based on size and per user group basis. It should also provide option to block object using MIME File types.
WSA.TR.26	The solution should allow administrator to define access to internet based on IP addresses, range of IP addresses, subnet and CIDR basis. It should also support to be forced for Authentication from Specific IP addresses, Subnet or CIDR's
WSA.TR.27	The solution should support Multiple Auth Servers / Auth Failover using Multi Scheme Auth (NTLM and LDAP). It should also support authentication exemption.
WSA.TR.28	The solution should support granular application control over web eg. Facebook controls like block file upload, block posting text, enforcing bandwidth limits on application types.
WSA.TR.29	Should support detection of Phone Home attempts occurring from the entire Network. It should also detect the PC's that are already infected with Malware in the Network across all network ports that attempts to bypass port 80.
WSA.TR.30	The solution should support providing bandwidth limit/cap for streaming media application traffic. This should be possible at the Global level as well as at a per policy level.
WSA.TR.31	The appliance should have support for at least 2 industry known Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Key loggers and as defined by the organizations policy. Please mention the antimalware engine.
WSA.TR.32	With dual AV/Anti-Malware engine scanning when a URL causes different verdicts from the scanning engine the appliance should perform the most restrictive action.
WSA.TR.33	The dual AV/Malware engines should protect at least against the follow types of malware/threats: Adware, Browser Helper Object, Commercial system monitor software's, Dialer, Generic spyware, Hijacker, Phishing

S. No.	Minimum Requirement Description
	URL, potentially unwanted applications, Trojan downloader, virus, worm etc.
WSA.TR.34	The solution should provide Web Reputation Filters that examine every request made by the browser (from
WSA.TR.35	the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web based score to determine the likelihood that it contains url-based malware.
WSA.TR.36	The Web Reputation Filters should have capability to analyze more than 100 different web traffic
WSA.TR.37	Network-related parameters to accurately evaluate the trustworthiness of a URL or IP address.
WSA.TR.38	Solution should also support in participating by providing information to the cloud based servers to increase the efficacy & reputation based scoring.
WSA.TR.39	The Appliance should have customizable setting in the Web Based Reputation Services, like Allow, Scan and Block based on the scoring settings by the Administrator.
WSA.TR.40	The solution should scan for Incoming and outgoing traffic.
WSA.TR.41	The solution shall provide option to scan all ports at wire speed, detecting and blocking spyware activity trying to connect to the outside Internet. By tracking all 65,535 network ports and all protocols, the solution shall effectively mitigate malware that attempts to bypass Port 80
WSA.TR.42	The solution should have an inbuilt URL filtering functionality with multiple pre-defined categories.
WSA.TR.43	The solution should support creation of custom URL categories for allowing/blocking specific destinations as required by the Organization.
WSA.TR.44	The web Proxy should support following actions like allow, monitor, block, time-based access. Should also support displaying a warning page but allows the user to continue clicking a hypertext link in the warning page.
WSA.TR.45	Provision should be available to enable Real Time Dynamic categorization that shall classify in real time in case the URL the user is visiting is not already under the pre-defined or custom categories database.
WSA.TR.46	The solution should have facility for End User to report Mis-categorization in URL Category.
WSA.TR.47	Support portal should give facility to end user to check URL category and submit new URL for categorization
WSA.TR.48	Solution should support filtering adult content from web searches & websites on search engines like google.
WSA.TR.49	The solution should support signature based application control. For instance, it should allow Facebook but should support blocking of only chat or file transfer or playing games within Facebook. This blocking should be based on signature and not URL. The application signature database should be updated periodically by the vendor. Mention the number of signatures available in the current release or mention the number of web based applications that can be blocked by the current signature set.
WSA.TR.50	Solution should support following end user notification functionalities.
WSA.TR.51	The proxy should support the functionality to display a custom message to the end user to specify the reason the web request is blocked.

S. No.	Minimum Requirement Description
WSA.TR.52	When the website is blocked due to suspected malware or URL-Filters it should allow the end user to report that the webpage has been wrongly misclassified.
WSA.TR.53	The solution should support the functionality of redirecting all notification pages to a custom URL to display a different block page for different reasons.
WSA.TR.54	Should support the functionality to force users to explicitly agree to the terms and conditions for browsing the World Wide Web from the organization's network to let the user know that the Organization is monitoring their web activity.
WSA.TR.55	The remote support from principal company should be available via India Toll Free and Email. The Support Portal access should be provided for Case management, knowledgebase, new version information, tools etc.
WSA.TR.56	The Support Engineers should be able to login to appliance using secure tunnelling methods such as SSH for troubleshooting purposes
WSA.TR.57	The appliance should have diagnostic network utilities like telnet, trace route, nslookup and tcpdump/packet capture.
WSA.TR.58	The appliance should provide seamless version upgrades and updates.
WSA.TR.59	Appliance should support a web interface that includes a tool that traces & can simulate client requests as if they were made by the end users and describes Web Proxy processes the request for troubleshooting purpose. It should support simulating HTTP GET & POST requests.
WSA.TR.60	The appliance should be manageable via HTTP or HTTPS
WSA.TR.61	The appliance should be manageable via command line using SSH
WSA.TR.62	For emergency, the appliance should have serial console access
WSA.TR.63	Should have provision for separate Ethernet for managing the appliance
WSA.TR.64	The Proxy Log should be scalable. The log formats shall include Apache, Squid and W3C.
WSA.TR.64	Solution should support automatic "rollover" & archive the log file when it reaches admin defined maximum file-size or time interval like daily/weekly rollover of logs.
WSA.TR.66	Should support compressing rolled over log files before storing them on disk to reduce disk space consumption.
WSA.TR.67	The appliance should support following mechanism to transfer log files:
WSA.TR.68	Should support remote FTP client to access the appliance to retrieve log files using an admin or operator user's username and password.
WSA.TR.69	Periodically pushing log files to an FTP server
WSA.TR.70	Periodically pushes log files using the secure copy protocol to an SCP server on a remote computer
WSA.TR.71	Sending logs to a remote syslog server confirming to RFC 3164.
WSA.TR.72	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP.
WSA.TR.73	Informative and exhaustive set of reports on User Activity and URL filtering activities (GUI to report past activity, top usage users and top malware threat)
WSA.TR.74	Reports on Bandwidth Consumed / Bandwidth Saved
WSA.TR.75	Product to maintain detailed proxy access logs that can be searched via filters, for easy location of any desired access of the user and to see how the product dealt with it

S. No.	Minimum Requirement Description
WSA.TR.76	Solution should also support centralized reporting.
WSA.TR.77	Detailed report on an IP basis should be provided on the L4 traffic monitoring / Network Layer Malware Detection.
WSA.TR.78	It should support reporting web requests blocked due to web reputation & blocked by malware
WSA.TR.79	Solution should support generating a printer-friendly formatted pdf version of any of the report pages. Should also support exporting reports as CSV files.
WSA.TR.80	Solution should support to schedule reports to run on a daily, weekly, or monthly basis.
WSA.TR.81	Should support system reports to show CPU usage, RAM usage, percentage of disk space used for reporting & logging.
WSA.TR.82	Support should cover all upgrades for the time period the licenses and support purchased from principal vendor
WSA.TR.83	Should have the ability to proxy, monitor, and manage IPv6 traffic.

#### 7.6.14 L3 Switch

S. No.	Nature of Requirement	Minimum Requirement Specifications
SWDC.REQ.001	Ports	24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports/FX Ports (splits as needed) and extra 2 numbers of Base-SX/LX ports
		All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports
SWDC.REQ.002	Switch type	Layer 3
SWDC.REQ.003	MAC	Support 8K MAC address
SWDC.REQ.004	Backplane	56 Gbps or more switching fabric capacity for 24 ports
		104 Gbps or more Switching fabric capacity for 48 ports
SWDC.REQ.005	Forwarding rate	Packet Forwarding Rate should be 70.0 Mbps or better
SWDC.REQ.006	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
SWDC.REQ.007	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
SWDC.REQ.008	Protocols	Support 802.1D, 802.1S, 802.1w, Rate limiting
		Support 802.1X Security standards
		Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping
		802.1p Priority Queues, port mirroring, DiffServ

S. No.	Nature of Requirement	Minimum Requirement Specifications
		<p>Support based on 802.1p priority bits with at least 8 queues</p> <p>DHCP support &amp; DHCP snooping/relay/optional 82/ server support</p> <p>Shaped Round Robin (SRR) or WRR scheduling support.</p> <p>Support for IPV6 ready features with dual stack</p> <p>Support up to 255 VLANs and up to 4K VLAN IDs</p> <p>Support IGMP Snooping and IGMP Querying</p> <p>Support Multicasting</p> <p>Should support Loop protection and Loop detection, Should support Ring protection</p>
SWDC.REQ.009	Access Control	<p>Support port security</p> <p>Support 802.1x (Port based network access control).</p> <p>Support for MAC filtering.</p> <p>Should support TACACS+ and RADIUS authentication</p>
SWDC.REQ.010	VLAN	<p>Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN</p> <p>The switch must support dynamic VLAN Registration or equivalent</p> <p>Dynamic Trunking protocol or equivalent</p>
SWDC.REQ.011	Protocol and Traffic	<p>Network Time Protocol or equivalent Simple Network Time Protocol support</p> <p>Switch should support traffic segmentation</p> <p>Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number</p>
SWDC.REQ.012	Management	<p>Switch needs to have RS-232/USB console port for management via a console terminal or PC</p> <p>Must have support SNMP v1,v2 and v3</p> <p>Should support 4 groups of RMON</p> <p>Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface</p>

### 7.6.15 24-Port PoE GE layer 2 Switch

S. No.	Minimum Requirement Description
	General Hardware and Interface requirements
L2S.TR.01	Switch should have minimum 24x10/100/1000Mbps PoE/PoE+ Ethernet Ports and 4x1G SFP uplink ports.
L2S.TR.02	Switch shall support minimum 80 Gbps of stacking bandwidth and stacking port should be dedicate port not uplink port
L2S.TR.03	Switch should support Redundant Power supply (Internal/External)
L2S.TR.04	Stacking module should be hot-swappable.
	Performance Requirements
L2S.TR.05	Switch shall have minimum 216 Gbps of switching fabric and 70 Mpps of forwarding rate.
L2S.TR.06	Switch shall have minimum 16 K MAC Addresses.
L2S.TR.07	Switch shall have minimum 1K Active VLANs.
L2S.TR.08	Switch shall support minimum 1K IPv4 and IPv6 unicast routes.
L2S.TR.09	Switch shall support minimum 1K IPv4 and IPv6 multicast groups.
L2S.TR.10	Switch shall support minimum 500 IPv4 and IPv6 QoS and Security ACLs.
L2S.TR.11	Switch must have atleast 512 Mb RAM and 128Mb Flash memory
	IEEE Standards
L2S.TR.12	Should support IEEE Standards of Ethernet: IEEE 802.1D, 802.1s, 802.1w, 802.1x, 802.3ad, 802.3x, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z.
	Quality of Service (QoS) requirements
L2S.TR.13	Switch shall have 802.1p class of service, IP differentiated service code point (DSCP) and cross stack QoS.
L2S.TR.14	Switch shall have committed information rate, rate limiting and flow based rate limiting.
L2S.TR.15	Switch shall have minimum 8 egress queues per port and strict priority queuing.
	System Management and Administration
L2S.TR.16	Switch should support SSHv2, SNMPv2c, SNMPv3, NTPv3 and NTPv4.
L2S.TR.17	Switch should support AAA using RADIUS and TACACS+.
L2S.TR.18	Switch should support port security, DHCP snooping, Dynamic ARP inspection, IP Source guard, BPDU Guard, Spanning tree root guard and IPv6 First Hop Security.
L2S.TR.19	Switch should support software upgrades via TFTP or FTP.
L2S.TR.20	Switch should support IPv4 and IPv6 ACLs, VLAN, Port and Time based access list with time ranges.
L2S.TR.21	Switch shall have Switch Port Analyzer (SPAN) and Remote Switch Port Analyzer (RSPAN).
L2S.TR.22	Switch shall have Layer 2 trace route for ease of troubleshooting by identifying the physical path that a packet takes from source to destination.
L2S.TR.23	Switch shall have Internet Group Management Protocol (IGMP) Snooping for IPv4 and IPv6, MLD v1 and v2 Snooping and Multicast VLAN Registration protocol.
L2S.TR.24	Switch shall have per port broadcast, multicast and unicast storm control.

S. No.	Minimum Requirement Description
L2S.TR.25	Switch shall have Unidirectional Link Detection Protocol (UDLD), Aggressive UDLD, Link Aggregation Control Protocol (LACP), Port Aggregation Protocol (PAgP) and Dynamic Trunking Protocol (DTP).
L2S.TR.26	Switch should be Software Defined Networking Ready with Open flow or similar protocol support
	Regulatory Compliance
L2S.TR.27	Switch shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 Standards for Safety requirements of Information Technology Equipment.
L2S.TR.28	Switch shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B Standards for EMC (Electro Magnetic Compatibility) requirements.
	Evaluation Compliance
L2S.TR.29	Switch should be IPv6 Certified/IPv6 logo ready.

#### 7.6.16 12-Port Layer 3 10G Switch (For Interconnecting)

S. No.	Minimum Requirement Description
	General Features
L3S.TR.01	Switch Should have 12 numbers of 10G SFP+ ports populated with multi-mode modules
L3S.TR.02	Should have Internal Redundant Power supply
L3S.TR.03	Switch should be based on a Modular OS Architecture capable of hosting applications.
L3S.TR.04	Switch should have USB 2.0 for OS Management (uploading, downloading & booting of OS and Configuration).
L3S.TR.05	Switch should have Multicore CPU Architecture.
L3S.TR.06	Should have at least 4GB of Flash for storing OS and other Logs and 4GB DRAM
L3S.TR.07	Switch should have Front to Back Airflow system and 3 number of field replaceable FAN's. In case of failure of one fan then other Fans should automatically speed-up
L3S.TR.08	Switch should have power savings mechanism wherein it should reduce the power consumption on ports not being used.
L3S.TR.09	Switch should be Rack Mountable and should not take space more than 1RU
	Performance
L3S.TR.10	Should have at least 280 Gbps switch fabric
L3S.TR.11	Forwarding rate - 210 Mbps at least
L3S.TR.12	Configurable at least 32000 MAC addresses
L3S.TR.13	Should support atleast 24K Ipv4 Routes Stacking/virtual chassis
L3S.TR.14	Switch should have dedicate stacking port and should support at least 8 number of switches in a single stack
L3S.TR.15	The Switch stack should be based on Distributed forwarding Architecture, where in each stack member forwards its own information on network.
L3S.TR.16	The Switch should support Stateful Switchover (SSO) when switching over from Active to Standby switch in a Stack.
L3S.TR.17	The Switch stacking module should be hot-swappable.
L3S.TR.18	The Switch stacking should support 320 Gbps of throughput.

S. No.	Minimum Requirement Description
L3S.TR.19	The Switch stacking should support automatic upgrade when master switch receives a new software version.
	Layer 3 Features
L3S.TR.20	The Switch should support routing protocols such OSPF, BGPv4, IS-ISv4, EIGRP
L3S.TR.21	The Switch should support IP Multicast routing protocol i.e PIM, PIM Sparse Mode, PIM Dense Mode, PIM Sparse-dense Mode & Source-Specific Multicast
L3S.TR.22	The Switch should have basic IP Unicast routing protocols (static, RIPv1 & RIPv2) and VRRP
L3S.TR.23	The Switch should have IPv6 & IPv4 Policy Based Routing (PBR) and Inter VLAN Routing
L3S.TR.24	The Switch should support uRPF for IPv4 and IPv6.
	Layer 2 Features
L3S.TR.25	The Switch should be able to discover (on both IPv4 & IPv6 Network) the neighbouring device giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems.
L3S.TR.26	The Switch should support Detection of Unidirectional Links (in case of fiber cut) and to disable them to avoid problems such as spanning-tree loops.
L3S.TR.27	The Switch should support centralized VLAN Management, VLANs created on the core switch should be propagated automatically.
L3S.TR.28	The Switch should support 802.3ad (LACP) to combine multiple network links for increasing throughput and providing redundancy.
	Network Security Features
L3S.TR.29	The Switch should have Port security to secure the access to an access or trunk port based on MAC address to limit the number of learned MAC addresses to deny MAC address flooding.
L3S.TR.30	The Switch should support Dynamic ARP inspection (DAI) to ensure user integrity by preventing malicious users from exploiting the insecure nature of ARP.
L3S.TR.31	The Switch should support IP source guard to prevent a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN.
L3S.TR.32	The Switch should support Unicast Reverse Path Forwarding (RPF) feature to mitigate problems caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address.
L3S.TR.33	The Switch should support flexible & multiple authentication mechanism, including 802.1X, MAC authentication bypass, and web authentication using a single, consistent configuration.
L3S.TR.34	The Switch should support Private VLANs to restrict traffic between hosts in a common segment by segregating traffic at Layer 2, turning a broadcast segment into a no broadcast multi-access like segment to provide security & isolation between switch ports, which helps ensure that users cannot snoop on other users' traffic.

S. No.	Minimum Requirement Description
L3S.TR.35	The Switch should support Spanning Tree Root Guard (STRG) to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
L3S.TR.36	The Switch should support IPv6 RA Guard, DHCPv6 guard, IPv6 Snooping to prevent any Man-in-middle attack.
L3S.TR.37	The Switch should support Dynamic VLAN, Downloadable ACLs, Multi-Auth VLAN Assignment, MAC Based Filtering & Web Authentication security mechanism.
	Operational features
L3S.TR.38	The Switch should support dynamic port and session configuration management.
L3S.TR.39	The Switch should support real-time network event detection and on-board automation in order to take informational, corrective actions when the monitored events occur (Embedded Event Manager).
	Quality of Service (QoS) & Control
L3S.TR.40	The Switch should support IP SLA feature set to verify services guarantee based on business critical IP Applications.
L3S.TR.41	The Switch should support Auto QoS for certain device types and enable egress queue configurations.
L3S.TR.42	The Switch should support Rate limiting based on source and destination IP address, source and destination MAC address, Layer 4 TCP/UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps.
	Application Visibility
L3S.TR.43	The Switch should support Full Flexible NetFlow v9 which provides ability to characterize IP traffic and identify its source, traffic destination, timing, and application information and is critical for network availability, performance, and troubleshooting.
L3S.TR.44	The Switch should be capable of enabling FnF on all ports of the switch for Ingress and Egress Traffic.
L3S.TR.45	The Switch should support atleast 24000 Flows per switch
L3S.TR.46	The Switch should support hop-by-hop analysis of application level statistics for troubleshooting video applications.
	Certification
L3S.TR.47	Switch should be EAL3/NDPP Certified

#### 7.6.17 Authentication, Authorization and Accounting (AAA) Specification)

S. No.	Minimum Requirement Description
AAA.TR.01	Proposed solution should be in leaders / challenger quadrant for Network Admission Control of Gartner's latest Magic quadrant
AAA.TR.02	The Solution should provide a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture, profiling and guest management services on a single platform.
AAA.TR.03	Solution should include all required licenses to perform above mentioned capabilities for 100 endpoints from day one and scalable to 5,000 in future. Additionally 400 endpoints licenses to be provided for AAA & Guest management only.

S. No.	Minimum Requirement Description
AAA.TR.04	It should allow enterprises to authenticate and authorize users and endpoints via wired, wireless, and VPN with consistent policy throughout the enterprise
AAA.TR.05	Proposed solution should include two appliances to be configured in Active/Standby
AAA.TR.06	Proposed solution should integrate with Firewall so that they learn identity information from access devices
AAA.TR.07	Should support enforcing security policies by blocking, isolating, and repairing noncompliant machines in a quarantine area without requiring administrator attention
AAA.TR.08	Should support improve network access control capabilities to identify, mitigate/quarantine and rapidly contain threats
AAA.TR.09	Should utilizes standard RADIUS protocol for authentication, authorization, and accounting (AAA).
AAA.TR.10	Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunnelling (FAST), and EAP-Transport Layer Security (TLS).
AAA.TR.11	Should provide a wide range of access control mechanisms, including downloadable access control lists (dACLs), VLAN assignments, URL redirect
AAA.TR.12	Should have predefined device templates for a wide range of endpoints, such as IP phones, printers, IP cameras, smartphones, IoT and tablets.
AAA.TR.13	It should allow Administrators to create their own device templates. These templates can be used to automatically detect, classify, and associate administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type.
AAA.TR.14	The Solution should have capability to collect endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the infrastructure via device sensors on switches.
AAA.TR.15	Should support capability to verify endpoint posture assessment for PCs connecting to the network. Should be a persistent client-based agent to validate that an endpoint is conforming to a smart city's posture policies. Provides the ability to create powerful policies that include but are not limited to checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), and applications.
AAA.TR.16	Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.
AAA.TR.17	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help-desk and network operators in quickly identifying and resolving issues. Offers comprehensive historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.
AAA.TR.18	Solution should support the following endpoint checks for compliance for windows endpoints: Check process, registry, file & application Check operating system/service packs/hotfixes

S. No.	Minimum Requirement Description
	check for Antivirus installation/Version/ Antivirus Definition Date check for Antispyware installation/Version/ Antispyware Definition Date Check for windows update running & configuration
AAA.TR.19	Proposed solution should support TACACS+ to simplify device administration and enhance security through flexible, granular control of access to network devices
AAA.TR.20	TACACS+ device administration should support: 1. Role-based access control 2. Flow-based user experience 3. Per Command level authorization with detailed logs for auditing
AAA.TR.21	Proposed solution should support capability to customize TACACS+ Services by specifying customer TACACS+ port number
AAA.TR.22	Proposed solution should support capability to create different network device groups so that administrator can create: 1. Different policy sets for IOS/OS or wireless controller OS 2. Different for firewall 3. Differentiate base on location of device
AAA.TR.23	Proposed solution should be able to create TACACS+ profile like Monitor, Privilege level, default, etc. to control the initial login session of device administrator.
AAA.TR.24	Proposed solution should be able to create TACACS+ authorization policy for device administrator containing specific lists of commands a device admin can execute. Command sets should support; exact match, case sensitive, (any character), * (matches any), etc. and support stacking as well
AAA.TR.25	Proposed solution must support TACACS+ in IPv6 network
AAA.TR.26	Solution should support receiving updated endpoint profiling policies and the updated OUI database as a feed from the OEM database.
AAA.TR.27	Should support Identity source sequences which defines the order in which the solution shall look for user credentials in the different databases. Solution should support the following databases:  •Internal Users, Internal Endpoints, Active Directory, LDAP, RSA, RADIUS Token Servers, Certificate Authentication Profiles
AAA.TR.28	Solution should have profiling capabilities integrated into the solution in order to detect headless host. The profiling features leverage the existing infrastructure for device discovery. Should support the use of attributes from the following sources or sensors: * Profiling using MAC OUIs * Profiling using DHCP information * Profiling using RADIUS information * Profiling using HTTP information * Profiling using DNS information / Nessus * Profiling using NetFlow information / On guard Agent * Profiling using SPAN/Mirrored traffic
AAA.TR.29	Should support troubleshooting & Monitoring Tools

### 7.6.18 Network Behaviour Analysis

S. No.	Minimum Requirement Description
NB.TR.01	Solution should provide a full-featured Network threat Analyzer capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.
NB.TR.02	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.
NB.TR.03	Should capture signature / heuristics based alerts and block the same
NB.TR.04	Should Identify the source of an attack and should not block legitimate users
NB.TR.05	Solution should have capability of retrieval of relevant packets to a cyber-security incident
NB.TR.06	Solution should perform lossless packet capture at rate of 1 Gbps of network traffic
NB.TR.07	Support importing/ exporting archived raw packets/files for analysis
NB.TR.08	Solution should Index all the data in the packets to simplify navigation across data silos and enable search-driven data discovery of packet metadata AND content for incident analysis
NB.TR.09	Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities
NB.TR.10	The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc.
NB.TR.11	Solution should detect common events like Scanning, Worms, Unexpected application services (e.g., tunneled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc.
NB.TR.12	Should utilize Anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration.
NB.TR.13	Solution should Integrate with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format
NB.TR.14	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANs
NB.TR.15	Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue
NB.TR.16	The system should be able to monitor flow data between various VLANs
NB.TR.17	Should support the capability to identify network traffic from high risk applications such as file sharing, peer-to-peer, etc.

S. No.	Minimum Requirement Description
NB.TR.18	Should support the capability to link usernames to IP addresses for suspected security events.
NB.TR.19	Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.
NB.TR.20	Should support the capability Application profiling in the system and should also support custom applications present or acquired by the bank/customer
NB.TR.21	Solution should be compatible with a virtual environment.
NB.TR.22	The reporting should be integrated with other network security systems (IPS, IDS, NAC, and Firewall etc.).
NB.TR.23	Solution should support capability to quarantine / remediate endpoint
NB.TR.24	Solution should be able to identify potential DDOS attacks originating from behind proxies.
NB.TR.25	Solution should be able to identify anomalies related to VOIP protocols over data network
NB.TR.26	Solution should be dedicated network behaviour analysis solution and not a subset of SIEM or Forensic analysis
NB.TR.27	Solution should support access to raw as well as processed logs
NB.TR.28	Solution should support built-in firewalling support, rejecting all packets by default (transparent to pings and port scans)
NB.TR.29	Dashboard should have the facility to be configured according to user profile
NB.TR.30	System should support event forwarding for SMTP, SYSLOG & SNMP for high risk issues
NB.TR.31	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.
NB.TR.32	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.
NB.TR.33	Solution should support ubiquitous access to view all reporting functions using an internet browser.
NB.TR.34	The solution should support the identification of applications tunnelling on other ports
NB.TR.35	Solution should be able to collect security and network information of servers and clients without the usage of agents
NB.TR.36	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance
NB.TR.37	The solution should have the ability to state fully reassemble unidirectional flows into bi-directional conversations; handling de-duplication of data and asymmetry
NB.TR.38	The solution should support all forms of flows including but not limited to netflow, juniper jflow, sflow, ipfix for udp etc.
NB.TR.39	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record

S. No.	Minimum Requirement Description
NB.TR.40	The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address
NB.TR.41	The solution should be able to leverage external threat feeds for information about known detection methods/fingerprints for Phishing, Botnets, Malware, Spyware, Connections to bad reputation Nations and Dark IP
NB.TR.42	Solution should support detection methods/fingerprints for Web crawler identification, location based threats & GEO IP based threats
NB.TR.43	The solution should be able to integrate with various SIEMs available in the market like RSA, Splunk, HP, etc
	Network performance
NB.TR.44	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption for top hosts and trends on network bandwidth utilization.
NB.TR.45	Dashboard should have the facility to be configured according to user profile
NB.TR.46	Solution should probe the network in a manner so that impact on network performance is minimal.
NB.TR.47	Should support both in line and offline modes.
NB.TR.48	The tool should have a system for interactive event identification and rule creation
NB.TR.49	Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.
NB.TR.50	Solution should have facility to assign risk and credibility rating to events.
NB.TR.51	Solution should support traffic rate up to 1 Gbps
NB.TR.52	Proposed flow collectors should have the ability to scale from 5000 flows per second scalable to 80000 flows per second in future
NB.TR.53	Proposed solution should be a dedicated appliance based solution

#### 7.6.19 SMS Gateway

S. No.	Minimum Requirement Description
SG.TR.001	Bidder has to provide SMS gateway of Telecom Service provider which has ability to withstand for continued growth in A2P SMS and support SVI_SMSG
SG.TR.003	The SMS gateway PULL SMS application must have security features to ensure confidentiality of sensitive customer data.
SG.TR.004	The SMS gateway PULL SMS application should be able to retrieve SMSs sent by devotees to one or more short codes / virtual numbers.
SG.TR.005	The SMS gateway PUSH SMS application should be able to send messages at different priority levels. In case the total number of messages to be sent exceeds the capacity promised, messages should be sent first as per higher priority and then following a FIFO rule. Other messages must be en-queued.
SG.TR.006	The SMS gateway PUSH SMS application must have the ability to set working hours and working days.

S. No.	Minimum Requirement Description
SG.TR.007	The Solution should offer configurable mechanism in terms of number of retries & time duration for each retry for messages that could not be delivered immediately.
SG.TR.008	Online Mechanism in real time mode has to be provided for SLA enforcement with regard to Uptime of Push /Pull services & Delivery of Push SMS along with flexibility to generate MIS on daily/weekly/fortnightly/monthly/specified date range basis.
SG.TR.009	The bidder should integrate with the Dashboard/Website/Portal for Administration features like monitoring of total messages sent within a day/ week/ month, time delay (if any) in sending the messages, no of failed messages (with reasons for failure), invalid mobile numbers, No of Push & Pull Messages sent.
SG.TR.010	The successful bidder shall demonstrate the Dashboard functionality & Reports format to SKVT before commissioning of SMS gateway services.
SG.TR.011	The bidder shall ensure that SMS whose contents exceeds 160 characters, should be delivered as a single message on receiver's handset.
SG.TR.012	The bidder should have proper test infrastructure with capability of end to end testing of all integration with SKVT Applications.
SG.TR.013	Check should be properly imposed to avoid Duplicate/ Multiple SMS Delivery to customers.
SG.TR.014	The solution should be capable of generating detailed report in Excel/ PDF. The solution should be capable of providing mobile-wise, Date-wise, category-wise reports and aggregated reports per category. The reports should contain timestamps of SMS received at Bidder's server , SMS Sent to the Telecom Operator, actual delivery to the end user & final status of SMS alert along with status description

#### 7.6.20 Fabric Controller

S. No.	Minimum Requirement Description
SDN.TR.01	Fabric is the Clos Architecture defined using Spine, Leaf and VXLAN + ISIS or VXLAN + EVPN Protocol
SDN.TR.02	Fabric should have following functionalities to be achieved:
SDN.TR.03	Flexibility : allows workload mobility anywhere in the DC
SDN.TR.04	Robustness : while dynamic mobility is allowed on any authorized location of the DC, the failure domain is contained to its smallest zone
SDN.TR.05	Performance: full cross sectional bandwidth (any-to-any) – all possible equal paths between two endpoints are active
SDN.TR.06	Deterministic Latency : fix and predictable latency between two endpoints with same hop count between any two endpoints, independently of scale
SDN.TR.07	Scalability: add as many Leaf as needed to achieve desired scale in terms of number of servers while maintaining the same oversubscription ratio everywhere inside the fabric.
	Fabric Features
SDN.TR.08	In the fabric the oversubscription ration of the connectivity between each leaf to SPINE switches should not be less than 4:1

S. No.	Minimum Requirement Description
SDN.TR.09	Fabric must support various Hypervisor encapsulations including VXLAN, NVGRE and 802.1q natively without any additional hardware/software or design change.
SDN.TR.10	The fabric architecture must be based on hardware VXLAN overlays to provide logical topologies that are abstracted from the physical infrastructure with no performance degradation. Fabric must support VXLAN Switching/Bridging and VXLAN Routing.
SDN.TR.11	Fabric must support Role Based Access Control in order to support Multi - Tenant environment.
SDN.TR.12	Fabric Spine switches should only connect to the leaf switches
SDN.TR.13	Fabric must integrate with different virtual machine manager and manage virtualize networking from the single pane of Glass - Fabric Controller/SDN Controller
SDN.TR.14	Fabric must integrate with best of breed L4 - L7 appliances and manage using single pane of glass - Fabric Controller / SDN Controller
SDN.TR.15	Fabric must act as single distributed layer 2 switch, Layer 3 router and Stateless distributed firewall etc
SDN.TR.16	Fabric must provide REST APIs from the Central management appliance/SDN Controller in order to integrate with best of breed Management, Monitoring, Hypervisor and Cloud automation & Orchestration software.
	Fabric Layer 2, Layer 3 and Misc. Features
SDN.TR.17	Fabric must support Layer 2 features like LACP, STP /RSTP /MSTP, VLAN Trunking, LLDP etc
SDN.TR.18	Fabric must support integrated Routing and Bridging at the leaf layer.
SDN.TR.19	Fabric must support multi chassis ether channel/MLAG i.e. Host connects to two different Leaf switches and form ether channel using LACP/NIC Teaming on Host
SDN.TR.20	Fabric must support Jumbo Frame upto 9K Bytes on 1G/10G/25G/40G/100G ports
	Fabric Security Features
SDN.TR.21	Fabric must support VM attribute based zoning and policy
SDN.TR.22	Fabric must support Micro Segmentation for the Virtualize and Non - Virtualize environment
SDN.TR.23	Fabric must support true multi - tenancy
SDN.TR.24	Fabric must have zero trust policy model for connected systems or hosts to help in protecting against any kind of attacks like Unauthorized Access, Man - in - the - middle - attack, Replay Attack, Data Disclosure, Denial of Service
SDN.TR.25	Fabric must act as a State-less distributed firewall with the logging capability
	Fabric Scale and Performance
SDN.TR.26	Fabric should support scale up and scale out without any service disruption
SDN.TR.27	Fabric must integrate with multiple Virtual Machine Managers (i.e. vCenter,SCVMM , Open Stack etc.) of different Hypervisors simultaneously

S. No.	Minimum Requirement Description
SDN.TR.28	Fabric must be capable of connecting 2 physical servers and scale to 5000 physical servers. Controller should be licensed for a minimum of 1000 dual socket Hosts (if solution is based on host based licensing)
SDN.TR.29	Fabric must support minimum of 4 Leaf switches and scale upto 200 Leaf switches without any design change.
SDN.TR.30	Fabric must support for 500 VRF/Private network without any additional component or upgrade or design change
SDN.TR.31	Fabric must scale from 1 Tenant to 32 Tenant without any additional component or upgrade or design change
SDN.TR.32	Fabric must integrate with minimum 3 Virtual Machine Manager (i.e. vCenter, SCVMM, Open Stack etc.) of different Hypervisors simultaneously and scalable to 5 in future with or without common orchestrator
SDN.TR.33	Fabric must support minimum of 2 Spine Switches and scale upto 6 Spine switches without any design change.
	Fabric management
SDN.TR.34	Fabric must provide Centralized Management Appliance or SDN Controller - Single pane of Glass for managing, monitoring and provisioning the entire Fabric.
SDN.TR.35	Fabric must Auto discover all the Spine and Leaf switches and auto provision them based on the Fabric policy using Centralized Management appliance or SDN Controller.
SDN.TR.36	Centralized management appliance or SDN Controller must manages and provision L4 - L7 Services physical or virtual appliance as well as integrate with Virtual Machine manager.
SDN.TR.37	Centralized management appliance or SDN Controller should not participate in Data plane and control plane path of the fabric.
SDN.TR.38	Centralized management appliance or SDN Controller must communicate to south bound devices using open standard protocol i.e. OPFLEX / OPENFLOW / OVSDB or using Device APIs.
SDN.TR.39	Centralized management appliance or SDN Controller must communicate with the south bound devices using more than one path i.e. in path connectivity and out of band management connectivity
SDN.TR.40	Centralized management appliance or SDN Controller provide dynamic device inventory of the Fabric as well as current network topology of the fabric. It must also validate the cabling connectivity and generate alarms in case of wrong or faulty connectivity.
SDN.TR.41	Centralized management appliance or SDN Controller must run in "N + 1" or "N + 2" redundancy to provide availability as well as function during the split brain scenario
SDN.TR.42	In Event of all Centralized management appliances or SDN Controllers fails, the fabric must function without any performance degradation and with the current configuration.
SDN.TR.43	Centralized management appliance or SDN Controller must support multi tenancy from management perspective and also provide Role Based Access Control per tenant for the tenant management.
SDN.TR.44	All infrastructure required by fabric controllers to support the listed scale, should be provided by the bidder
SDN.TR.45	Architecture should be designed with respect to high availability.

S. No.	Minimum Requirement Description
SDN.TR.46	All the switches, fabric controller and Optics should be from same OEM
SDN.TR.47	Bidder must quote appropriate licenses to enable and meet all the above mentioned features and scale in the fabric specification

## 7.7 Generic IT Hardware

### 7.7.1 Keyboard and Joystick

S. No.	Nature of requirement	Minimum Requirement Description
JYT.TR.001	General	The control board shall be based upon standard components and proven technology
JYT.TR.002	Controller	Shall be equipped with Keypad for selecting desired cameras/ as per user configurations
JYT.TR.003	General	Shall be equipped with Jog dial for Viewing recording.
JYT.TR.004	Technical	Joystick: Pan Tilt and Zoom function
JYT.TR.005	Interface	USB 1.1/2.0/3.0 compliant
JYT.TR.006	Power	Via USB
JYT.TR.007	General	The control board shall be of modular design and provide keypad, joystick and jog dial functionality
JYT.TR.008	General	The inter-connectable modules shall be backed by an open and published API and shall, when combined with a video management application
JYT.TR.009	Keypad	Shall be equipped with 22 keys: 10 application defined hotkeys of which 5 are backlit, 0-9, TAB, ALT
JYT.TR.010	Jog dial	6 application defined hotkeys
JYT.TR.011	Joystick	Hall-effect joystick with three axis: a. X/Y: for pan and tilt b. Z: knob for zoom C. 6 application defined hotkeys
JYT.TR.012	General	The following features to be available; vector-solving, with twisting, return to-centre head
JYT.TR.013	Operating Cycle for Joystick	> 5,000,000 cycles or better
JYT.TR.014	Deflection	Square delimiter Pan/Tilt (XY): ±15° Zoom (Z): ±25°
JYT.TR.015	Casing	Polycarbonate
JYT.TR.016	Compatibility	Shall support all cameras and video servers
JYT.TR.017	Operating System Supported	Windows 7 or Later or Any other Operating system
JYT.TR.018	Certification	EN, CE, FCC, IEC
JYT.TR.019	Operating conditions	0 °C to 60 °C
JYT.TR.020	Operating Humidity	20% to 80% (RH)

S. No.	Nature of requirement	Minimum Requirement Description
JYT.TR.021	Warranty	5 years

### 7.7.2 Video Wall

S. No.	Nature of Requirement	Minimum Requirements
VIDWL.TR.01	Configuration	VIDEO WALL CUBES OF 50" DIAGONAL
VIDWL.TR.02	Cube & Controller	Cube & Controller should be from the same manufacturer
VIDWL.TR.03	Reputed Company	The OEM should be an established multinational in the field of video walls
VIDWL.TR.04	Native Resolution	Full HD ( 1920x 1080 )
VIDWL.TR.05	Light Source Type	Laser light source with Laser diodes
VIDWL.TR.06		Individual cube should be equipped with multiple laser banks and each laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen
VIDWL.TR.07	Brightness of Projection engine	Minimum 2000 lumens
VIDWL.TR.08	Brightness of Cube	Minimum 800 nits and should be adjustable for lower or even higher brightness requirements
VIDWL.TR.09	Brightness Uniformity	$\geq 98\%$
VIDWL.TR.10	Dynamic Contrast	1000000:1 or more
VIDWL.TR.11	Dust Prevention	Should meet or exceed IP6X standard. Certificate to this effect to be furnished from 3rd party Laboratory
VIDWL.TR.12	Control	IP based control to be provided
VIDWL.TR.13	Remote	IR remote control should also be provided for quick access
VIDWL.TR.14	Screen to Screen Gap	$\leq 1\text{ mm}$
VIDWL.TR.15	Screen Support	Screen should be minimum 3 layers with a Hard Backing to prevent bulging
VIDWL.TR.16	Control BD Input terminals	Input: 1 x Digital DVI
VIDWL.TR.17		Input: 1 x HDMI
VIDWL.TR.18		Input: 1 x Display Port
VIDWL.TR.19		Input: 1 x HDBase T
VIDWL.TR.20	Power Supply	Dual Redundant and Hot Swappable Power Supply. This should be built inside the cube for fail safe operation. Power supplies extended or kept outside the cube are not acceptable
VIDWL.TR.21	Cooling Inside Cube	By suitable method. Hazardous liquids inside the cooling system are not acceptable
VIDWL.TR.22	Cube Depth	Total Cube depth including screen module should be less than 450 mm or lower
VIDWL.TR.23		Internal Temperature

S. No.	Nature of Requirement	Minimum Requirements
VIDWL.TR.24	Monitoring of critical parameters to ensure stable operation of the system 24 x 7	Ambient Temperature
VIDWL.TR.25		Humidity
VIDWL.TR.26		Brightness
VIDWL.TR.27		Cooling
VIDWL.TR.28		Light Source Status
VIDWL.TR.29		Should be possible to demonstrate these parameter through an active monitoring interface
VIDWL.TR.30	Maintenance Access	Cube should be accessible from the front side to save space
VIDWL.TR.31	Cube Size	
VIDWL.TR.32	Cube control & Monitoring	Video wall should be equipped with a cube control & monitoring system
VIDWL.TR.33		Should be able to control & monitor individual cube , multiple cubes and multiple video walls
VIDWL.TR.34		Provide video wall status including Source , light source ,temperature, fan and power information
VIDWL.TR.35		Should provide a virtual remote on the screen to control the video wall
VIDWL.TR.36		System should have a quick monitor area to access critical functions of the video wall

### 7.7.3 PC – ICCC

S. No.	Nature of Requirement	Minimum Requirements
PC1.TR.001	Processor	Intel Core i7-4770processor @ 3.5 Hz
PC1.TR.002	RAM	32 GB
PC1.TR.003	Internal storage	1 TB SATA 3.0Gb/s
PC1.TR.004	Network Interface	2x10/100/1000
PC1.TR.005	Graphics	NVIDIA ® GeForce ® GTX 1060 or equivalent
PC1.TR.006	Display	3 Nos 24" LED screen Full HD
PC1.TR.007	Keyboard & Mouse	USB based
PC1.TR.008	Port	Minimum 4 Nos USB ports
PC1.TR.009	Operating System	Pre-loaded OS latest

### 7.7.4 PC – DC & Help desk

S. No.	Nature of Requirement	Minimum Requirements
PC1.TR.001	Processor	Intel Core i7-4770processor @ 3.5 Hz
PC1.TR.002	RAM	32 GB

PC1.TR.003	Internal storage	1 TB SATA 3.0Gb/s
PC1.TR.004	Network Interface	2x10/100/1000
PC1.TR.005	Graphics	NVIDIA ® GeForce ® GTX 1060 or equivalent
PC1.TR.006	Display	3 Nos 21" LED screen Full HD
PC1.TR.007	Keyboard & Mouse	USB based
PC1.TR.008	Port	Minimum 4 Nos USB ports
PC1.TR.009	Operating System	Pre-loaded OS latest

#### 7.7.5 Printer

S. No.	Nature of requirement	Minimum Requirement Description
PRINT.TR.01	General	Printers shall be of latest laser technology & for duplex printing (colour and black and white) for all paper size including but not limited to A4, A3 size.
PRINT.TR.03	Technical	It shall have Print Speed 30ppm or above.
PRINT.TR.04	Technical	It shall have Resolution Min 600 x 600 dpi or better.
PRINT.TR.05	Technical	It shall have Memory 1 GB or higher.
PRINT.TR.06	Technical	It shall have Copy speed 12ppm or better.
PRINT.TR.07	General	It shall have scanner of Flat Bed type with ADF.
PRINT.TR.08	Technical	It shall have Interface USB 2.0, Ethernet Port.
PRINT.TR.09	General	It shall have the duty cycle of monthly 5000 pages at minimum.
PRINT.TR.10	General	Full toner Cartridge shall be supplied with the printer.
PRINT.TR.11	General	It shall have input tray capacity of minimum 100 sheets.
PRINT.TR.12	General	It shall have output tray capacity of minimum 100 sheets.
PRINT.TR.13	General	Printer shall be accompanied with the necessary accessories such as connecting cables, driver media, etc.

#### 7.7.6 Desktop

S. No.	Nature of requirement	Minimum Requirement Description
DT.TR.01	Processor	Intel Core i7 , 64bit x86 Processor @ 3.2 GHz or more, 4MB L3 cache, Memory support DDR3 or better specifications
DT.TR.02	Motherboard & Chipset	OEM Motherboard
DT.TR.03	Video	Integrated Graphic controller
DT.TR.04	Network	Integrated 10 / 100 / 1000 Gigabit Ethernet controller

S. No.	Nature of requirement	Minimum Requirement Description
DT.TR.05	Ports	1 HDMI port (Preferable), 2x USB 2.0 and 2 x USB 3.0 (Preferable), 10 USB ports external - with minimum 4 ports USB 3.0 Front I / O includes (2 or more ) USB 2.0 ports Rear I / O includes (2 or more ) USB 3.0 ports, (2 or more) USB 2.0 ports, serial port, Parallel port, PS 2 mouse and keyboard ports, RJ-45 network interface, Display Port 1 VGA and 3.5mm audio in /out jacks; 4 in 1 Media Card Reader (Preferable)
DT.TR.06	HDD Controller	Integrated dual port SATA-II controller
DT.TR.07	Memory	8GB DDR III 1333MHz or higher expandable up to 16 GB or more
DT.TR.08	Storage	1TB @ HDD 7200 RPM
DT.TR.09	Optical Drive	22X DVD writer or higher and the corresponding software
DT.TR.10	Monitor	21" TFT LCD touch screen monitor minimum 1920 x 1080 resolution with 5 ms response time or better specifications, TCO 03 or higher certified
DT.TR.11	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard
DT.TR.12	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 cpi, Complying to CE and FCC norms
DT.TR.13	Power Management and DMI	System with Power management features & Desktop Management Interface implementation
DT.TR.14	Operating System	Supported by Windows, Linux etc.
DT.TR.15	Power input	100 -240V AC
DT.TR.16	Certifications	EPEAT
DT.TR.17	Graphic Card	Extra Graphic card for support Visuals

#### 7.7.7 IP Camera Surveillance

S. No.	Minimum Technical Specifications
IPCS.TR.001	Entire area of the Data Centre is covered using IP Camera Video Surveillance, Recording and Replay facilities. Bidder shall provide (a)Fixed dome cameras as per BOM
IPCS.TR.002	IP camera system to provide an online display of colour video images on monitor where the entire set up is monitored from the control room on a 24X7 basis. Suitable camera lenses are used to view critical area such as Data centre, Reception and corridor.
IPCS.TR.003	Use of fixed dome cameras with remote controlled focus and zoom controlled from control room.
IPCS.TR.004	Dome camera unit to be Colour Dome camera in an integrated dome and base unit, wall or ceiling mountable.
IPCS.TR.005	Cabling solution for IP Surveillance to include all necessary cabling between cameras and video management/recording systems

S. No.	Minimum Technical Specifications
IPCS.TR.006	System should provide cable termination facilities, cable distribution system for video and power system along with any additional video amplifiers. All necessary relay boxes, connectors and extension cables
IPCS.TR.007	Visual images captured are fed into the centralized Video Management/Recording system that can be viewed on monitors in BMS/Control room.
IPCS.TR.009	A minimum of 30 days inbuilt recording facility. Suitable internal hard disk with raid to be provisioned by the bidder as part of solution
IPCS.TR.010	Outdoor cameras shall be day/night cameras with sufficient Zoom correction for various light variations
IPCSTR.011	All outdoor cameras are to be IP 66 rated
IPCS.TR.012	Necessary functionalities on the camera lenses to avoid internal condensation or condensation on the windows
IPCS.TR.015	Provide playback at a rate of up to 400 FPS
IPCS.TR.016	Minimum of 8 or more video inputs with looping
IPCS.TR.018	Allow digital zoom during playback
IPCS.TR.019	Support for simultaneous playback and recording
IPCS.TR.020	Ability to back up recorded data to hard disk or DVD
IPCS.TR.021	Device to support at least 1 number of 10/100/1000 Ethernet port for LAN connectivity

## 7.8 Non - IT Hardware

### 7.8.1 Fire Alarm System

S. No.	Minimum Requirements
FPDS.TR.001	The Fire system shall deploy High Sensitivity Smoke/ Heat Detectors (HSSD) and Very Early Smoke Detection Appliance (VESDA) to allow swift detection of heat and/or smoke. The System shall consist of a high sensitive smoke detector, aspirator, and filter
FPDS.TR.002	Solution must conform to Code of Practices approved by agencies such as Bureau of Indian Standards (BIS), British Standards Institution (BSI) or National Fire Protection Association (NFPA), CE. The alarms shall be monitored on a 24 x 7 basis & logged for providing reports.
FPDS.TR.003	Microprocessor controlled single loop control panel with Multi Zone, multi device 2 wire detection loop, Break glass units on escape routes and exits.
FPDS.TR.004	The control panel shall have an integral automatic power supply and maintenance free sealed battery, providing a standby capacity of a minimum 72 hours and further 30 minutes under full alarm load conditions.
FPDS.TR.005	Fire detection system shall be designed for three levels -
FPDS.TR.006	a. Below raised Floor
FPDS.TR.007	b. Room void

S. No.	Minimum Requirements
FPDS.TR.008	c. Above false ceiling - using analogue addressable fire detection system
FPDS.TR.009	The detector must provide different environmental algorithms that allow the detector to provide superior false alarm immunity without the need for additional alarm verification delays.
FPDS.TR.010	It shall be required to establish cross zoning across the server hall so as to ensure the accuracy of the alarm sensed and minimise false alarms. Once, minimum of two zones sense an alarm, the fire alarm should be designed to cut power to air-conditioning system, cut all the power supply to the NOC and release access for all the entry and exit points. The fire suppression system should be triggered off after a pre-set time interval.
FPDS.TR.011	Multiple Smoke Threshold Alarm Levels.
FPDS.TR.012	Indication of faults including airflow, detector, power, filter block and network as well as an indication of the priority/ urgency of the fault.
FPDS.TR.013	Configurable relay outputs for remote indication of alarm and fault conditions.
FPDS.TR.014	Fire Control system status shall be made available via panel mounted LED's and an alpha numeric LCD display
FPDS.TR.015	All system controls and programming to be possible through an alpha numeric key pad
FPDS.TR.016	Ability for fire control panel to record events, faults and historic logs giving time, date and device reference.
FPDS.TR.017	The detector shall have a multicolour LED to ease/ streamline system maintenance/inspection by plainly indicating detector status as follows: green for normal operation, amber for minor alarm/ maintenance required, red for major alarm.
FPDS.TR.018	The intelligent smoke detector shall be capable of providing three distinct outputs from the control panel. The outputs shall be from an input of smoke obscuration, a thermal condition or a combination of obscuration and thermal conditions. The detector shall be designed to eliminate calibration errors associated with field cleaning of the chamber.
FPDS.TR.019	Thermal Detectors shall be rated at 135 degrees Fahrenheit fixed temperature and 15 degrees per minute rate of rise. Detectors shall be constructed to compensate for the thermal lag inherent in conventional type detectors due to the thermal mass and alarm at the set point of 135 degrees Fahrenheit.
FPDS.TR.020	Detector bases shall be low profile twist lock type with screw clamp terminals and self-wiping contacts. Bases shall be installed on an industry standard, 4" square or octagonal electrical outlet box.
FPDS.TR.021	The notification appliance shall be audible/visual appliance or equivalent. Notification appliance shall be electronic and use solid state components.
FPDS.TR.022	Each electronic appliance shall provide multiple field selectable alarm tones.

S. No.	Minimum Requirements
FPDS.TR.023	The appliance shall provide at least two output sound levels: STANDARD and HIGH dBA.
FPDS.TR.024	The combination audible/ visual appliances shall be installed indoors and may be surface or flush mounted. They shall mount to standard electrical hardware requiring no additional trim plate or adapter. The aesthetic appearance shall not have any mounting holes or screw heads visible when the installation is completed
FPDS.TR.025	Novec 1230 system shall be UL listed.
FPDS.TR.026	Fire Suppression solution should conform to best in class NFPA and other standards
FPDS.TR.027	The fire suppression agent should
FPDS.TR.028	- Not contain Ozone Depleting Substances
FPDS.TR.029	- Not produce Toxic by products
FPDS.TR.030	- ODP of 0
FPDS.TR.031	- Adherence to Kyoto protocol
FPDS.TR.032	The clean agent fire suppression system with FK-5-1-12 and Inert Gas based systems are accepted as a replacement of HCFC and HFC as per Kyoto Protocol.
FPDS.TR.033	The fire suppression system shall include and not be limited to gas release control panel, UL listed Seamless PESO approved Cylinders, discharge valve, discharge pipe, non-return valve and all other accessories required to provide a complete operational system meeting applicable requirements of NFPA 2011 and installed in compliance with all applicable requirements of the local codes and standards.
FPDS.TR.034	Fire Suppression systems shall deploy cross zoned detector systems for all locations to ensure suppression only in affected areas
FPDS.TR.035	Portable Extinguishers (CO2) shall be placed at strategic stations throughout the NOC
FPDS.TR.036	Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling and below false floor. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm.
FPDS.TR.037	The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
FPDS.TR.038	Primary controls shall be password protected over 4 access levels in accordance with EN54 Part 2.
FPDS.TR.039	Audible/visual appliance or equivalent
FPDS.TR.040	Multiple Feedback selectable alarm tones - HORN, BELL, MARCH, MARCH TIME HORN, CODE-3 HORN, CODE-3 TONE, SLOW WHOOP, SIREN and HI/LO, etc.
FPDS.TR.041	Multiple sound output levels with standard and HIGH Db levels

S. No.	Minimum Requirements
FPDS.TR.042	The re-fill facility for gas cylinders should be done at UL Listed refilling centre only.
FPDS.TR.043	Provide new version upgrades, updates, patches, etc. for all the components / sub-components through the period of contract

### 7.8.2 Rodent Repellent System

S. No.	Minimum Specification Requirements
RRR.TR.001	Entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be installed in the false ceiling to repel the pests without killing them.
RRR.TR.002	Periodic pest control using Chemical spray shall be done once in 3 months as a contingency measure to effectively fight the pest menace. Treatment to protect against termites and other pests shall be done using "Imidacloprid spray" all over the data centre area once every six months during O&M phase and at the time of completion of implementation phase.
RRR.TR.003	The rodent control system should comprise of an Ultrasonic Pest Repellent of a VFHO Model. The repellents shall be provided in false flooring and ceiling. System panel shall be configured with main Building Management/ Energy Management System.

### 7.8.3 Air-conditioned 2 Ton

S. No.	Nature of requirement	Minimum Requirements
CAC2.TR.001	Make & Model	Bidder to Specify
CAC2.TR.002	Capacity	2 tonnage
CAC2.TR.003	Star Rating	5 star/invertor
CAC2.TR.004	Cooling Capacity	Minimum 5000 W
CAC2.TR.005	Noise Level (Indoor) dBA	45/28
CAC2.TR.006	Noise Level (Outdoor) dBA	53
CAC2.TR.007	Compressor	Dual Rotary or equivalent
CAC2.TR.008	Panel Display	Digital
CAC2.TR.009	Operating mode	Swing mode
CAC2.TR.010	Condenser Coil	Copper
CAC2.TR.011	Power requirement	AC 230 V, 50 Hz
CAC2.TR.012	Power Consumption	Average 2000 W
CAC2.TR.013	Refrigerant Type	R410A or equivalent
CAC2.TR.014	Warranty	1 year for product

#### 7.8.4 Centralized Cooling System

Centralize cooling system is required for Police Control centre, Municipal operation centre, NOC room, War room, DG room and common area of the Integrated Command and Control Centre.

S. No.	Nature of Requirement	Specification
CCS-TR-01	Standard Features	R-410A chlorine-free refrigerant
CCS-TR-02		High-efficiency scroll compressors
CCS-TR-03		Two-stage cooling
CCS-TR-04		Copper tube / aluminium fin coils (7½ - 10 Ton)
CCS-TR-05		Micro-Channel indoor & outdoor coils (12½ Ton)
CCS-TR-06		Power block for field wiring
CCS-TR-07		High- and low-pressure switches
CCS-TR-08		High-capacity, steel-cased filter drier
CCS-TR-09		Heater kits with single-point entry
CCS-TR-10		24-volt terminal strip
CCS-TR-11	Performance	Units meet the performance outlined in Table 6.8.1-1 of ASHRAE Standard 90.1-2013
CCS-TR-12	Certification	AHRI Certified; ETL Listed
CCS-TR-13	Cabinet Features	Heavy-gauge, galvanized steel cabinet with UV-resistant powder-paint finish
CCS-TR-14		Built-in filter rack with standard 2" filters
CCS-TR-15		Convertible airflow orientation
CCS-TR-16		Easy to service
CCS-TR-17		Full perimeter rail
CCS-TR-18		Sloped drain pan
CCS-TR-19	Powered Convenience Outlet	A GFCI outlet powered with a transformer shall be built into the unit. Powered convenience outlet shall be installed in the equipment. The MOP (Max. Overcurrent Protection) device must be sized accordingly.
CCS-TR-20	Non-powered Convenience Outlet	A 120V, 15A, GFCI outlet makes it easier for technicians to service the unit once an electrician runs power to the outlet.
CCS-TR-21	Economizers (Down flow)	Based on air conditions, can provide outside air to cool the space.
CCS-TR-22	Electric Heat Kits	Available in all voltage options
CCS-TR-23	Phase Monitor	Phase monitor (3 phase only), available for 3 - 25 ton DS, DC and DT series models. Phase monitor shall provide protection for motors and compressors against problems caused by phase loss, phase reversal and phase unbalance. Phase monitor is equipped with an LED that provides an ON or FAULT indicator.
CCS-TR-24	DDC Controller	DDC communicating controller, available for 3 - 25 ton DS, DC and DT series models with on-board BACnet communication interface.

### 7.8.5 HVAC – PAC

S. No.	Nature of requirement	Minimum Requirements
PAC.TR.001	General Features Design	Microprocessor based Precision Air conditioning system. Cooling shall be done by the Precision Air-Conditioning system only
PAC.TR.002		24*7 operations design
PAC.TR.003		Cool air feed to the server farm shall be bottom-charged or downward flow type using raised floor as supply plenum using perforated aluminium tiles for Air flow distribution
PAC.TR.008		3 independent refrigeration circuits for server room and minimum refrigeration circuit for UPS room
PAC.TR.009		The return air flow shall be through false ceiling/below false ceiling to cater to the natural upwardly movement of hot air.
PAC.TR.010		Forced cooling using Fans on False floor etc. is not acceptable.
PAC.TR.011		Capable of providing sensible cooling capacities at design ambient temperature & humidity with adequate airflow.
PAC.TR.012		The PAC should capable to be integrated with the Building management System for effective monitoring with the ability to send alarms for temperature and humidity variations
PAC.TR.013		
PAC.TR.014		
PAC.TR.015		Is the proposed product/solution End-of-life or shall reach End-of-life within 48 months from the date of submission of bid?
PAC.TR.016		Provide new version upgrades, updates, patches, etc. for all the components / sub-components through the period of contract
PAC.TR.017	Make and Model	Bidder to specify
PAC.TR.018	Type	Dx based PAC units ( Stand-alone without any Chiller water feed )
PAC.TR.019	Air Discharge	Through EC Plug Fan
PAC.TR.020	Design Condition	Temp/RH
PAC.TR.021		(28 ± 2° C / 40% RH~60 % RH at return air of Precision AC
PAC.TR.022	Sensible heat ratio at above design conditions	Bidder to specify

S. No.	Nature of requirement	Minimum Requirements
PAC.TR.023	General Features Design	Air filters to prevent particulate clogging shall be deployed that shall operate at 95% efficiency & provide up-to 5 Micron particulate/ grade EU4 shall be deployed
PAC.TR.024		Proportional Integration Differential PID control of Temperature and humidity
PAC.TR.025		The unit casing shall be in double skin construction on the side panels & single skin on the front & back panels for longer life of unit
PAC.TR.026		Dual blowers for flexibility of operations and better redundancy.
	COMPRESSOR	
PAC.TR.027	Scroll design	Multiple scroll Compressors for server room and single scroll compressor for UPS room
PAC.TR.028	Coolant	R410A/R407C refrigerant
PAC.TR.029	Anti-vibration mountings	Anti-vibration mounting to be made available
	EVAPORATOR COIL	
PAC.TR.030	Face Area	Bidder to specify
PAC.TR.031	Face Velocity in FPM	Bidder to specify
PAC.TR.032	Hydrophilic coating on coil	Yes
	EVAPORATOR FAN	
PAC.TR.033	Type of Fan	Aluminium backward curved Direct driven EC Plug Fan
PAC.TR.034	Fan Power in KW/TR	Bidder to Specify
PAC.TR.035	No. of Fan and Fan Diameter	Bidder to specify
	FILTERS	
PAC.TR.036	Air filter specification	90~95%/5Micron/grade EU4
	HUMIDIFIERS	
PAC.TR.037	Type	Electrode Type/Infrared
PAC.TR.038	Capacity in Kg/hr	Bidder to specify
PAC.TR.039	Power in KW	Bidder to specify
	HEATERS	
PAC.TR.040	Capacity in KW	Bidder to specify
PAC.TR.041	Number of Stages	Minimum Two
PAC.TR.042	Whether safety thermostat manual provided	YES
PAC.TR.043	with reset	

S. No.	Nature of requirement	Minimum Requirements
	MICROPROCESSOR CONTROLLER	
PAC.TR.044	No. of Potential free contact available for external communication	Bidder to Specify
PAC.TR.045	Status updates	Status updated for Temperature, Compressor, Blower fan, Humidifier
PAC.TR.046	Control points for operation	Establish control mechanism to initiate actions for
PAC.TR.047		- Cooling capacity control
PAC.TR.048		- Compressor starting timer
PAC.TR.049		- Humidifier capacity limitation
PAC.TR.050		- Date and time of alarm history
PAC.TR.051		- Random starting of the unit
PAC.TR.052		- Temperature and humidity set point calibration
PAC.TR.053		- Start / Stop status storage
PAC.TR.054		- Delay of General Alarm activation
PAC.TR.055		- Alarm Display in Microprocessor unit for clogged filters
	UNIT CASING	
PAC.TR.056	Type of panel	All side panels shall be double skinned sandwich panel with fire retention insulation inside with GI Sheet / Powder Coated and CRCA / powder Coated
PAC.TR.057		Panels are coated inside with PU foam for sufficient insulation thickness
	ELECTRICAL	
PAC.TR.058	Isolation for incoming	To be ensured
PAC.TR.059	Fuse for individual motors	To be ensured
PAC.TR.060	Terminal strip for all connection with cable marking	To be ensured
PAC.TR.061	Single phase preventers	To be ensured
PAC.TR.062	Low Voltage / High Voltage cut off	To be ensured
PAC.TR.063	Phase reversal protection	To be ensured
	INSTRUMENTATION	

S. No.	Nature of requirement	Minimum Requirements
PAC.TR.064	Sensors for	To be ensured
PAC.TR.065	Return air temperature	To be ensured
PAC.TR.066	Return air humidity	To be ensured
PAC.TR.067	Supply air	To be ensured
PAC.TR.068	Auto restart after power resumption	To be ensured
PAC.TR.069	Cascading and Team Mode	YES
PAC.TR.070	Sound level at 1.5m distance in dBA	75
	ACCESSORIES	
PAC.TR.071	Unit mounting stand	To be ensured
PAC.TR.072	Return air damper	To be ensured
PAC.TR.073	Drain piping	To be ensured
	Microprocessor	
PAC.TR.074	Integration with BMS	To be ensured
PAC.TR.075	Control	Synchronising the units to work as a single system and this feature to be provided in every unit controller
PAC.TR.076		Working or standby configuration to be possible in the controller.
PAC.TR.077		Multiple units shall be possible to connect in team mode for power savings and this feature shall be provided in the each unit to provide high uptime
PAC.TR.078		Cascading feature - in case of high load standby unit to get ON automatically and once the room conditions are met standby unit to off automatically
PAC.TR.079		Should have clog filter, Airflow loss, Water leak detection, sequencing, possibility to connect to fire alarm sensors etc.
	Nominal Dimensions	
PAC.TR.080	Length in mm	To be Specified by Bidder
PAC.TR.081	Width in mm	To be Specified by Bidder
PAC.TR.082	Height in mm	To be Specified by Bidder
PAC.TR.083	Net/Operating Weight (Approximate) in kg	To be Specified by Bidder

### 7.8.6 Transformer

S. No.	Nature of requirement	Minimum Requirement Description
TRFMR.TR.01	Supply Type	3 Phase A.C.
TRFMR.TR.02	Use Type	Outdoor
TRFMR.TR.03	Distribution Rating	250 KVA
TRFMR.TR.04	System voltage (Max.)	12 KV
TRFMR.TR.05	Rated Voltage (HV)	11 KV
TRFMR.TR.06	Rated Voltage (LV)	433 - 250 V* *The voltage level can be specified as 433/415-250 volts as per the requirements of the purchaser.
TRFMR.TR.07	Frequency	50 Hz +/- 5%*
TRFMR.TR.08	No. of Phases	Three
TRFMR.TR.09	Connection HV	Delta Type
TRFMR.TR.10	Connection LV	Star (Neutral brought out)
TRFMR.TR.11	Vector group	Dyn-11
TRFMR.TR.12	Type of cooling	ONAN
TRFMR.TR.13	Voltage Level	433/415-250 volts
TRFMR.TR.14	Core Material	The core shall be stack / wound type of high grade Cold Rolled Grain Oriented or Amorphous Core annealed steel lamination having low loss and good grain properties, coated with hot oil proof insulation, bolted together and to the frames firmly to prevent vibration or noise.  The transformers core shall be suitable for over fluxing (due to combined effect of voltage and frequency) up to 12.5% without injurious heating at full load conditions and shall not get saturated.  No-load current up to 200kVA shall not exceed 3% of full load current and shall be measured by energising the transformer at rated voltage and frequency. Increase of 12.5% of rated voltage shall not increase the no-load current by 6% of full load current.
TRFMR.TR.15	Winding Material	HV and LV windings shall be wound from Super Enamel covered /Double Paper covered Aluminium / Electrolytic Copper conductor.  Inter layer insulation shall be Nomex /Epoxy dotted Kraft Paper.
TRFMR.TR.16	Oil	The insulating oil shall comply with the requirements of IS 335. Use of recycled oil is not acceptable. The specific resistance of the

S. No.	Nature of requirement	Minimum Requirement Description
		<p>oil shall not be less than <math>35 \times 10^{12}</math> ohm-cm at <math>27^\circ\text{C}</math> when tested as per IS 6103.</p> <p>Oil shall be filtered and tested for break down voltage (BDV) and moisture content before filling.</p> <p>The oil shall be filled under vacuum.</p>
TRFMR.TR.17	Insulation Levels	<p>Voltage (kV) - 0.433, Impulse Voltage (kV Peak) - , Power Frequency Voltage (kV) - 3</p> <p>Voltage (kV) - 11, Impulse Voltage (kV Peak) - 75 , Power Frequency Voltage (kV) - 28</p> <p>Voltage (kV) - 33, Impulse Voltage (kV Peak) - 170 , Power Frequency Voltage (kV) - 70</p>
TRFMR.TR.18	Tolerances	No positive tolerance shall be allowed on the maximum losses displayed on the label for both 50% and 100% loading values.
TRFMR.TR.19	Temperature Rise	<p>The temperature rise over ambient shall not exceed the limits given below:</p> <p>Top oil temperature rise measured by thermometer : <math>35^\circ\text{C}</math></p> <p>Winding temperature rise measured by resistance method : <math>40^\circ\text{C}</math></p> <p>The transformer shall be capable of giving continuous rated output without exceeding the specified temperature rise.</p>
TRFMR.TR.20	Insulation Material	<p>Electrical grade insulation epoxy dotted Kraft Paper/Nomex and pressboard of standard make or any other superior material</p> <p>All spacers, axial wedges / runners used in windings shall be made of pre-compressed Pressboard-solid, conforming to type B 3.1 of IEC 641-3-2.</p>
TRFMR.TR.21	Plain Tank	<p>The transformer tank shall be of robust construction rectangular/octagonal/round/ elliptical in shape and shall be built up of electrically tested welded mild steel plates of thickness of 3.15 mm for the bottom and top and not less than 2.5 mm for the sides for distribution transformers up to and including 25 kVA, 5.0 mm and 3.15 mm respectively for transformers of more than 25 kVA and up to and including 100 kVA and 6 mm and 4 mm respectively above 100 kVA. Tolerances as per IS1852 shall be applicable.</p> <p>In case of rectangular tanks above 100 kVA the corners shall be fully welded at the corners from inside and outside of the tank to</p>

S. No.	Nature of requirement	Minimum Requirement Description
		<p>withstand a pressure of 0.8 kg/cm<sup>2</sup> for 30 minutes</p> <p>Under operating conditions the pressure generated inside the tank should not exceed 0.4 kg/ sq. cm positive or negative. There must be sufficient space from the core to the top cover to take care of oil expansion. The space above oil level in the tank shall be filled with dry air or nitrogen conforming to commercial grade of IS 1747.</p> <p>The tank shall be reinforced by welded flats on all the outside walls on the edge of the tank.</p> <p>The permanent deflection, when the tank without oil is subjected to a vacuum of 525 mm of mercury for rectangular tank and 760 mm of mercury for round tank, shall not be more than the values as given below:</p> <p>Horizontal length of flat plate Up to and including 750 : 5.0, 751 to 1250 : 6.5, 1251 to 1750 : 8.0, 1751 to 2000 : 9.0</p> <p>The tank shall further be capable of withstanding a pressure of 0.8kg/sq.cm and a vacuum of 0.7 kg/sq.cm (g) without any deformation.</p> <p>The radiators can be tube type or fin type or pressed steel type to achieve the desired cooling to limit the specified temperature rise.</p>
TRFMR.TR.22	Corrugated Tank	<p>The transformer tank shall be of robust construction corrugated in shape and shall be built up of tested sheets.</p> <p>Corrugation panel shall be used for cooling. The transformer shall be capable of giving continuous rated output without exceeding the specified temperature rise. Bidder shall submit the calculation sheet in this regard.</p> <p>Tanks with corrugations shall be tested for leakage test at a pressure of 0.25kg/ sq cm measured at the top of the tank.</p> <p>The transformers with corrugation should be provided with a pallet for transportation, the dimensions of which should be more than the length and width of the transformer tank with corrugations.</p>
TRFMR.TR.23	Conservator	Transformers of rating 63 kVA and above with plain tank construction, the provision of conservator is mandatory. For corrugated

S. No.	Nature of requirement	Minimum Requirement Description
		tank and sealed type transformers with or without inert gas cushion, conservator is not required. When a conservator is provided, oil gauge and the plain or dehydrating breathing device shall be fitted to the conservator which shall also be provided with a drain plug and a filling hole [32 mm (1¼ ")] normal size thread with cover. In addition, the cover of the main tank shall be provided with an air release plug.
		The dehydrating agent shall be silica gel. The moisture absorption shall be indicated by a change in the colour of the silica gel crystals which should be easily visible from a distance. Volume of breather shall be suitable for 500g of silica gel conforming to IS 3401 for transformers up to 200 kVA and 1 kg for transformers above 200 kVA.
		The capacity of a conservator tank shall be designed keeping in view the total quantity of oil and its contraction and expansion due to temperature variations. The total volume of conservator shall be such as to contain 10% quantity of the oil. Normally 3% quantity the oil shall be contained in the conservator.
		The cover of main tank shall be provided with an air release plug to enable air trapped within to be released, unless the conservator is so located as to eliminate the possibility of air being trapped within the main tank.
		The inside diameter of the pipe connecting the conservator to the main tank should be within 20 to 50 mm and it should be projected into the conservator so that its end is approximately 20 mm above the bottom of the conservator so as to create a sump for collection of impurities. The minimum oil level (corresponding to -5 OC) should be above the sump level.
TRFMR.TR.24	Surface Preparation and Painting	All paints, when applied in a normal full coat, shall be free from runs, sags, wrinkles, patchiness, brush marks or other defects. All primers shall be well marked into the surface, particularly in areas where painting is evident and the first priming coat shall be applied as soon as possible after cleaning. The paint shall be applied by airless spray according to manufacturer's

S. No.	Nature of requirement	Minimum Requirement Description
		<p>recommendations. However, where ever airless spray is not possible, conventional spray be used with prior approval of purchaser.</p> <p>Steel surfaces shall be prepared by shot blast cleaning (IS9954) to grade Sq. 2.5 of ISO 8501-1 or chemical cleaning including phosphating of the appropriate quality (IS 3618).</p> <p>Chipping, scraping and steel wire brushing using manual or power driven tools cannot remove firmly adherent mill-scale. These methods shall only be used where blast cleaning is impractical. Manufacturer to clearly explain such areas in his technical offer.</p>
TRFMR.TR.25	Protective Coating	<p>As soon as all items have been cleaned and within four hours of the subsequent drying, they shall be given suitable anti-corrosion protection.</p> <p>Following are the types of paint which may be suitably used for the items to be painted at shop and supply of matching paint to site: Heat resistant paint (Hot oil proof) for inside surface</p> <p>For external surfaces one coat of thermo setting powder paint or one coat of epoxy primer followed by two coats of synthetic enamel/polyurethane base paint. These paints can be either air drying or stoving.</p> <p>For highly polluted areas, chemical atmosphere or for places very near to the sea coast, paint as above with one coat of high build Micaceous iron oxide (MIO) as an intermediate coat may be used.</p>
TRFMR.TR.26	Bushings	<p>The bushings shall conform to the relevant standards specified and shall be of outdoor type. The bushing rods and nuts shall be made of brass material 12 mm diameter for both HT and LT bushings. The bushings shall be fixed to the transformers on side with straight pockets and in the same plane or the top cover for transformers above 100 kVA. For transformers of 100 kVA and below the bushing can be mounted on pipes. The tests as per latest IS 2099 and IS 7421 shall be conducted on the transformer bushings.</p> <p>For 33 kV, 52 kV class bushings shall be used for transformers of ratings 500 kVA and</p>

S. No.	Nature of requirement	Minimum Requirement Description
		<p>above. And for transformers below 500 KVA, 33 kV class bushings, for 11 kV, 17.5 kV class bushings and for 0.433 kV, 1.1 kV class bushings shall be used.</p> <p>Bushing can be of porcelain/epoxy material. Polymer insulator bushings conforming to relevant IEC can also be used.</p> <p>Bushings of plain shades as per IS 3347 shall be mounted on the side of the Tank and not on top cover.</p> <p>Dimensions of the bushings of the voltage class shall conform to the Standards specified and dimension of clamping arrangement shall be as per IS 4257.</p> <p>Arcing horns shall be provided on HV bushings.</p> <p>Brazing of all inter connections, jumpers from winding to bushing shall have cross section larger than the winding conductor. All the Brazes shall be qualified as per ASME, section - IX.</p> <p>The bushings shall be of reputed make supplied by those manufacturers who are having manufacturing and testing facilities for insulators.</p> <p>The terminal arrangement shall not require a separate oil chamber not connected to oil in the main tank.</p>
TRFMR.TR.27	Terminal Connectors	<p>The LV and HV bushing stems shall be provided with suitable terminal connectors as per IS 5082 so as to connect the jumper without disturbing the bushing stem. Connectors shall be with eye bolts so as to receive conductor for HV. Terminal connectors shall be type tested as per IS 5561.</p>
TRFMR.TR.28	Lightning Arrestors	<p>9 kV, 5 kA metal oxide lightning arrestors of reputed make conforming to IS 3070 Part-III, one number per phase shall be provided. (To be mounted on pole or to be fitted under the HV bushing with GI earth strip 25x4 mm connected to the body of the transformer with necessary clamping arrangement as per requirement of purchaser.) Lightening arrestors with polymer insulators in conformance with relevant IEC can also be used.</p>
TRFMR.TR.29	Cable Boxes	In case HV/LV terminations are to be made through cables the transformer shall be fitted

S. No.	Nature of requirement	Minimum Requirement Description
		<p>with suitable cable box on 11 kV side to terminate one 11kV/ 3 core aluminium conductor cable up to 240 sq. mm. (Size as per requirement).</p> <p>The bidder shall ensure the arrangement of HT Cable box so as to prevent the ingress of moisture into the box due to rain water directly falling on the box. The cable box on HT side shall be of the split type with faces plain and machined and fitted with Neo-k-Tex or similar quality gasket and complete with brass wiping gland to be mounted on separate split type gland plate with nut-bolt arrangement and MS earthing clamp. The bushings of the cable box shall be fitted with nuts and stem to take the cable cores without bending them. The stem shall be of copper with copper nuts. The cross section of the connecting rods shall be stated and shall be adequate for carrying the rated currents. On the HV side the terminal rod shall have a diameter of not less than 12 mm. The material of connecting rod shall be copper. HT Cable support clamp should be provided to avoid tension due to cable weight.</p>
		<p>The transformer shall be fitted with suitable LV cable box having non-magnetic material gland plate with appropriate sized single compression brass glands on LV side to terminate 1.1 kV/single core XLPE armoured cable (Size as per requirement).</p>
TRFMR.TR.30	Terminal Markings	<p>High voltage phase windings shall be marked both in the terminal boards inside the tank and on the outside with capital letter 1U, 1V, 1W and low voltage winding for the same phase marked by corresponding small letter 2u, 2v, 2w. The neutral point terminal shall be indicated by the letter 2n. Neutral terminal is to be brought out and connected to local grounding terminal by an earthing strip.</p>
TRFMR.TR.31	Fittings	<p>The following standard fittings shall be provided :</p> <ul style="list-style-type: none"> <li>i. Rating and terminal marking plates, non-detachable.</li> <li>ii. Earthing terminals with lugs - 2 Nos.</li> <li>iii. Lifting lugs for main tank and top cover</li> <li>iv. Terminal connectors on the HV/LV bushings (For bare terminations only).</li> </ul>

S. No.	Nature of requirement	Minimum Requirement Description
		<p>v. Thermometer pocket with cap - 1 No.</p> <p>vi. Air release device</p> <p>vii. HV bushings - 3 Nos.</p> <p>viii. LV bushings - 4 Nos.</p> <p>ix. Pulling lugs</p> <p>x. Stiffener</p> <p>xi. Radiators - No. and length may be mentioned (as per heat dissipation calculations)/ corrugations.</p> <p>xii. Arcing horns or 9 kV, 5 kA lightning arrestors on HT side - 3 No.</p> <p>xiii. Prismatic oil level gauge.</p> <p>xiv. Drain cum sampling valve.</p> <p>xv. Top filter valve</p> <p>xvi. Oil filling hole having p. 1- 1/4 " thread with plug and drain plug on the conservator.</p> <p>xvii. Silicagel breather</p> <p>xviii. Base channel 75x40 mm for up to 100 kVA and 100 mmx50 mm above 100 kVA, 460 mm long with holes to make them suitable for fixing on a platform or plinth.</p> <p>xix. 4 No. rollers for transformers of 200 kVA and above.</p> <p>xx. Pressure relief device or explosion vent.</p>
TRFMR.TR.32	Fastners	<p>All bolts, studs, screw threads, pipe threads, bolt heads and nuts shall comply with the appropriate Indian Standards for metric threads, or the technical equivalent.</p> <p>Bolts or studs shall not be less than 6 mm in diameter except when used for small wiring terminals.</p> <p>All nuts and pins shall be adequately locked.</p> <p>Wherever possible bolts shall be fitted in such a manner that in the event of failure of locking resulting in the nuts working loose and falling off, the bolt shall remain in position.</p> <p>All ferrous bolts, nuts and washers placed in outdoor positions shall be treated to prevent corrosion, by hot dip galvanising, except high tensile steel bolts and spring washers which shall be electro-galvanised/plated.</p> <p>Appropriate precautions shall be taken to prevent electrolytic action between dissimilar metals.</p> <p>Each bolt or stud shall project at least one thread but not more than three threads through the nut, except when otherwise</p>

S. No.	Nature of requirement	Minimum Requirement Description
		approved for terminal board studs or relay stems. If bolts and nuts are placed so that they are inaccessible by means of ordinary spanners, special spanners shall be provided.
		The length of the screwed portion of the bolts shall be such that no screw thread may form part of a shear plane between members.
		Taper washers shall be provided where necessary.
		Protective washers of suitable material shall be provided front and back of the securing screws.
TRFMR.TR.33	Overload Capacity	The transformers shall be suitable for loading as per IS 6600.

#### 7.8.7 LT Distribution Panel

S. No.	Nature of requirement	Minimum Requirement Description
LTDP.TR.01	Atmospheric Conditions	<ul style="list-style-type: none"> <li>a) Maximum temperature of air in shade : 45°C</li> <li>b) Minimum temperature of air in shade : 0°C</li> <li>c) Maximum temperature of air in sun : 50°C</li> <li>d) Maximum humidity : 100%</li> <li>e) Average number of thunder storm days per annum : 70 days</li> <li>f) Average number of dust storm days per annum : 20 days</li> <li>g) Maximum rainfall per annum : 2000 mm</li> <li>h) Average rainfall per annum : 1500 mm</li> <li>i) Maximum ambient temperature daily average : 45°C</li> <li>j) Wind pressure : 200Kg/M2</li> <li>k) Altitude : Less than 1000m</li> </ul>
LTDP.TR.02	Material	Distribution Cabinets shall be outdoor type.
		These shall be fabricated out of 2 mm CR sheet steel duly acid treated and finished with one coat anticorrosive primer and two coats of grey epoxy paint.
		The body of the boxes shall have sufficient reinforcement with suitable size of channels keeping a provision for fixing these boxes either on DP structure or plinths.
		The Box shall have double door with locking arrangement and a door handle conforming to IS 8623/1977.
		The roof of the box shall be slightly slanting both

S. No.	Nature of requirement	Minimum Requirement Description
		<p>sides with an overhang of 50mm to the front and back side.</p> <p>The nuts, bolts, washers used in the box shall be galvanized to avoid rusting.</p> <p>The door hinges shall not be visible from outside.</p> <p>The box shall have a solid earthing point and arrangement for sufficient ventilation.</p> <p>The boxes should confirm to IP 54 degree of protection.</p> <p>The box shall have provision of bus bars of Electrolytic Cooper mounted on epoxy resin cast bus insulators fixed on suitable fixing arrangement.</p> <p>The bus bars shall be conveniently placed so as to provide adequate clearance from the body of the box conforming to I.E. Rules applicable for L.T. supply.</p> <p>There should be heat shrinkable bus bar insulation tubing on the busbars.</p>
LTDP.TR.03	KIT KAT FUSE UNIT	<p>Shall be of reputed make as per IS-2086</p> <p>The kit kats should have 500 V rating.</p> <p>All contact parts are plated and made of copper and brass with A class porcelain with extended terminal fitted with slots hex bolts with nuts.</p>
LTDP.TR.04	MCCB	<p>i) Standard : IS 13947 (Part-2) /1993 &amp; IEC Pub -947 -2 (1989)</p> <p>ii) Rated voltage : 415 vol. Ac</p> <p>iii) No. of poles : 3</p> <p>iv) Utilisation category : A</p> <p>v) Rated service short circuit breaking capacity: The percentage of rated service short circuit breaking capacity (I.Cs) to rated ultimate circuit breaking capacity (icu) shall be mentioned as per IS 13947 (Part-2) /1989.</p> <p>vi) Type of protection: Overload protection is a must with static /electromagnetic /thermo magnetic trip release.</p> <p>vii) The terminal capacity of the MCCBs should be such as to accommodate the required LT cable. The incoming cable should be connected to the terminals of the M.C.C.B. with Bi- metallic lugs duly crimped with Die press &amp; crimping tools. There should be a metallic /heat resistant insulating barrier between the MCCB side &amp; that of kit kat fuses so that the heat generated in Kit Kat fuses</p>

S. No.	Nature of requirement	Minimum Requirement Description
		carrying current and during fuse blow should not pass to the MCCB.
LTDP.TR.05	General	The distribution boxes shall be duly wired with suitable size of PVC insulated single core copper cable or equivalent section copper/aluminium flat.
		Terminal connectors for the earth connections to be provided in the box.
		The distribution cabinet should be preferably of IP-54 protective category, with provision for lighting inside the cabinet.

#### 7.8.8 Lighting

S. No.	Nature of requirement	Minimum Requirement Description
LIGHT.TR.01	General	All overhead lighting shall be LEDs both recessed direct and indirect lighting, including pot-lights.
LIGHT.TR.02	General	The overhead lighting treatment shall be incorporated into the other ceiling elements to create an aesthetic specialty ceiling design, in combination with the Rooms.
LIGHT.TR.03	Technical	Overhead lighting intensity shall be:
		• For Command & Control Center: at least 400 lux
		• For City Operation Center: at least 400 lux
		• For War Room: at least 500 lux
		• For Server Farm Area: at least 500 lux
		• UPS Room: at least 500 lux
		• BMS Room: at least 500 lux
LIGHT.TR.04	Technical	• NOC Room: at least 500 lux
		Dimming control shall be continuous (all lights dimmable) and zone-based (with a minimum of 4 lighting zones on separate circuits).
LIGHT.TR.05	Technical	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.)
LIGHT.TR.06	General	Appropriate wall boxes for corresponding dimmer size shall be provided.
LIGHT.TR.07	General	Dimmers shall not be ganged in one box.
LIGHT.TR.08	General	Manual switches shall be used for on / off lighting control and for overriding any preset lighting configurations.
LIGHT.TR.09	General	Cover plates for switches shall match the colour of switches, receptacles, and receptacle cover plates. Cover plates shall be of the same manufacturer as the devices.

S. No.	Nature of requirement	Minimum Requirement Description
LIGHT.TR.10	General	All lighting fixtures shall be of high-grade quality over and above the standard level of quality for office lighting.
LIGHT.TR.11	General	Lighting arrangement shall accommodate console locations.
LIGHT.TR.12	General	Lighting shall be configured in order to reduce glares and reflections on console monitors and on the video wall, as well as accommodate any other lighting needs the monitors and video wall may have.

#### 7.8.9 Diesel Generator 250KVA

S. No.	Nature of requirement	Minimum Requirements
DG.TR.001	Support	Is the proposed product/solution End-of-life or shall reach End-of-life within 48 months from the date of submission of bid?
DG.TR.002		Provide new version upgrades, updates, patches, etc. for all the components / sub-components throughout the period of contract
DG.TR.003		Shall the proposed product/solution reach End-of-support during the first 10 years after submission of this bid?
DG.TR.004	Dimension and Weight (With canopy)	Bidder to specify
DG.TR.005	Diesel Engine	Diesel Engine water cooled suitable for Generating Set application with canopy
DG.TR.006		overload capacity of 10% for one hour in any 12 hours of continuous operation
DG.TR.007		Engine should be selected on the basis of prime engine rating.
DG.TR.008	Capacity	Bidder to specify
DG.TR.009	Total Quantity	(Suitable for required Prime Output of the coupled Generator set at 0.8 PF.)
DG.TR.010	Redundancy configuration	Shall be able to be configured for Redundancy from two phases
DG.TR.011	Accessories	Bidder to specify
DG.TR.012	No. of cylinders	Multi-Cylinders. Turbo-Charged
DG.TR.013	Speed in RPM	Bidder to Specify
DG.TR.014	Controls	Automatic 'stop' device if any parameters are varied beyond upper/lower limits Integral mounted of instrument panel complete with wiring (For engine) & connections
DG.TR.015	Fuel tank & fuel Piping	Fuel tank to be located within 10 meter periphery of the DG set

S. No.	Nature of requirement	Minimum Requirements
DG.TR.016	Type of governor	Electronic, Class 1
DG.TR.017	Type of lubrication	Lube oil
DG.TR.018	Whether heat exchanger is provided	YES
	Alternator	
DG.TR.020	Capacity in KVA	200 KVA Self-excited, competent for parallel operation with droop CT & kit
DG.TR.021	Alternator	The alternator shall be self-excited, self-regulated, self-ventilated in brush less for suitable automatic voltage regulator and shall conform to BS: 2613 or equivalent standard and shall give rated output at NTP conditions. The alternator shall have space heater which shall be connected with breaker NO/NC contacts and this should be able to cut off with thermostat. The alternator shall have RTD and BTD
DG.TR.022	Enclosure	Sound proof, drip proof & screen protected (minimum as per IP: 23). The alternator terminal box shall be amended and made suitable for bus duct arrangement.
DG.TR.023	Other Specifications of Alternator	As per rated, Self-excited, self-regulated foot mounted fitted with ball and roller bearings and having PMG(preferred), RTD, BTD, space heater, 3 nos. differential CTs or REF CTs or both differential and REF CTs depending on rating, 1 no. earth fault CT, droop CT for paralleling.
DG.TR.024	Speed	1500 rpm
DG.TR.025	Acoustics	The acoustic treatment shall ensure a maximum sound pressure not more than 68 dB (A) at 1 meter during the day and 45 dB (A) at the neighbour's premises during night, while running on partial or full load. This condition shall apply to the engine exhaust noise levels also. A vertical type "Critical" silencer shall be fitted on the Exhaust pipe.
DG.TR.026	Class of insulation	Class H
DG.TR.027	Bearings	Heavy duty pre-lubricated
DG.TR.028	Ventilation	Centrifugal fan
DG.TR.029	Terminal	Bus duct arrangement with Flange for termination and provision of differential /REF CT's
DG.TR.030	Voltage Regulation	+/- 1.5% all load between no load to full load & power factor 0.8 to unity.
DG.TR.031	Overload Capacity	10% for one hour in any 12 hours of operation without exceeding temperature rise limits specified in BS: 2613 when corrected to ambient temperature at site
DG.TR.032	Space Heater to be provided	Yes

S. No.	Nature of requirement	Minimum Requirements
DG.TR.033	Total Losses as % of rated KW	Not more than 4
DG.TR.034	Efficiency in %	Not less than 80
DG.TR.035	Type of bearing	Single
DG.TR.036	Exciter details	Bidder to specify
DG.TR.037	AVR details & voltage adjustment	Bidder to specify
DG.TR.038	DG enclosure	Enclosure for DG set using MS frame cladded with 0.47 GI sheet with powder coated

#### 7.8.10 UPS 60 KVA

S. No.	Nature of Requirement	Minimum Requirement Description
UPS.TR.001	Capacity	60 KVA
UPS.TR.002	Input Range	415V/230V, 3 wire
		Frequency 50 HZ ±3 HZ
UPS.TR.003	Output Voltage & Waveform	415V/230V, 3 wire
UPS.TR.004	Input & Output Power Factor	Input Power Factor > 0.9 Output Power Factor > 0.8
UPS.TR.005	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand
UPS.TR.006	Frequency	50 Hz +/- 0.5% (free running), Pure Sine wave
UPS.TR.007	Crest Factor	Min. 3:1 at full load
UPS.TR.008	Third Harmonic Distribution	< 3%
UPS.TR.009	Input Harmonic Level	< 10%
UPS.TR.010	Overall Efficiency	Min. 90% on Full Load
UPS.TR.011	Noise Level	< 55 dB @ 1 meter
UPS.TR.012	Backup	at least 30 minutes
UPS.TR.013	Warranty	3 years with UPS & 2 years for battery
UPS.TR.014	Certification	ISO 9001:2008 & ISO 14001 certified
UPS.TR.015	Protection	To be provided for overload/ short circuit; overheating; input over/ under voltage; output over/ under voltage.
UPS.TR.016	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection

S. No.	Nature of Requirement	Minimum Requirement Description
UPS.TR.017	Interface	SNMP interface support (for remote monitoring)
UPS.TR.018	Galvanic Isolation	To be provided through Inbuilt transformer
UPS.TR.019	Compatibility	UPS to be compatible with DG Set supply and mains supply
UPS.TR.020	Bypass	Automatic Bypass Switch
UPS.TR.021	Technology	True ON-LINE (Double Conversion) with IGBT based rectifier and inverter and PWM Technology
UPS.TR.022	Support	Support for min. 5 years
UPS.TR.023	Operating Temperature	5 to 55 Degrees Centigrade
UPS.TR.024	Enclosure	CE certified
UPS.TR.025	Mandatory Compliance	BIS , ROHS
UPS.TR.026	Safety Certificate	IEC 62040-1

#### 7.8.11 UPS 20 KVA

S. No.	Nature of requirement	Minimum Requirement Description
UPS.TR.001	Capacity	20 KVA
UPS.TR.002	Input Range	415V/230V, 3 wire
		Frequency 50 HZ ±3 HZ
UPS.TR.003	Output Voltage & Waveform	415V/230V, 3 wire
UPS.TR.004	I/P & O/P Power Factor	0.9 or higher power factor
UPS.TR.005	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand
UPS.TR.006	Frequency	50 Hz +/- 0.5% (free running), Pure Sine wave
UPS.TR.007	Crest Factor	Min. 3:1 at full load
UPS.TR.008	Third Harmonic Distribution	< 3%
UPS.TR.009	Input Harmonic Level	< 10%
UPS.TR.010	Overall Efficiency	Min. 90% on Full Load
UPS.TR.011	Noise Level	< 55 db @ 1 Meter
UPS.TR.012	Backup	at least 30 minutes
UPS.TR.013	Warranty	3 years with UPS & 2 yrs for battery
UPS.TR.014	Certification	ISO 9001:2008 & ISO 14001 certified

S. No.	Nature of requirement	Minimum Requirement Description
UPS.TR.015	Protection	To be provided for overload/ short circuit; overheating; input over/ under voltage; output over/ under voltage.
UPS.TR.016	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection
UPS.TR.017	Interface	SNMP interface support (for remote monitoring)
UPS.TR.018	Galvanic Isolation	To be provided through Inbuilt transformer
UPS.TR.019	Compatibility	UPS to be compatible with DG Set supply and mains supply
UPS.TR.020	Bypass	Automatic Bypass Switch
UPS.TR.021	Technology	True ON-LINE (Double Conversion) with IGBT based rectifier and inverter and PWM Technology
UPS.TR.022	Support	Support for min. 5 years
UPS.TR.023	Operating Temperature	5 to 55 Degrees Centigrade
UPS.TR.024	Enclosure	CE certified
UPS.TR.025	Mandatory Compliance	BIS , ROHS
UPS.TR.026	Safety Certificate	IEC 62040-1

#### 7.8.12 Projector

S. No.	Nature of requirement	Minimum Requirement Description
PROJ.TR.01	General	3D Capable : Yes
PROJ.TR.02	General	Analog Video Signal : RGB, component video
PROJ.TR.03	General	Brightness : 4000 lumens
PROJ.TR.04	General	Colour Support : 1.07 billion colours
PROJ.TR.05	General	Contrast Ratio: 2200:1 / 10000:1 (dynamic)
PROJ.TR.06	General	Device Type: Projector with High Definition 720p or better display
PROJ.TR.07	General	Features : 2x colour wheel
PROJ.TR.08	General	Interfaces : 1 x VGA input - 15 pin HD D-Sub (HD-15)
PROJ.TR.09	General	Lamp Life Cycle : Up to 3000 hour(s) / up to 5000 hour(s) (economic mode)
PROJ.TR.10	General	Lamp Type: 260 Watt
PROJ.TR.11	General	Lens Aperture: F/2.4-2.66
PROJ.TR.12	General	Min Operating Temperature : 41 °F
PROJ.TR.13	General	Max Operating Temperature : 104 °F
PROJ.TR.14	Projector	Native Aspect Ratio: 0.67361
PROJ.TR.15	Projector	Output Power / Channel : 10 Watt
PROJ.TR.16	Projector	Power: AC 230 V (50 Hz)
PROJ.TR.17	Projector	Projection Distance: 4 ft. - 33 ft.
PROJ.TR.18	Lens	Resolution: WXGA (1280 x 800)

S. No.	Nature of requirement	Minimum Requirement Description
PROJ.TR.19	Lens	Security Features: Security lock slot
PROJ.TR.20	Lens	Sound Emission: 37 dB
PROJ.TR.21	Video Input	Sound Emission (Economic Mode): 32 dB
PROJ.TR.22	Video Input	Sound Output Mode: Mono
PROJ.TR.23	Video Input	Speakers: Speaker(s) - integrated
PROJ.TR.24	Speakers	Speakers: 1 x mixed channel
PROJ.TR.25	Speakers	Throw Ratio: 1.28 - 1.536:1
PROJ.TR.26	Speakers	TV System: PAL-B/G, PAL-N, PAL-M, PAL-I, NTSC 4.43, NTSC 3.58, PAL-D, SECAM L, PAL-H, SECAM K1, SECAM D/K, SECAM B/G
PROJ.TR.27	Speakers	Type: Integrated
PROJ.TR.28	Expansion / Connectivity	Uniformity: 0.8
PROJ.TR.29	Miscellaneous	Video Input: RGB, component video (PAL-B/G, PAL-N, PAL-M, PAL-I, NTSC 4.43, NTSC 3.58, PAL-D, SECAM L, PAL-H, SECAM K1, SECAM D/K, SECAM B/G)
PROJ.TR.30	Environmental Parameters	Video Interfaces: VGA, HDMI
PROJ.TR.31	Environmental Parameters	Video Modes: 480p, 720p, 1080i, 1080p, 480i, 576i, 576p
PROJ.TR.32	Environmental Parameters	Zoom Factor: 1.2x
PROJ.TR.33	Environmental Parameters	Zoom Type: Manual

## 7.9 Helpdesk Hardware

### 7.9.1 IP phone

S. No.	Nature of requirement	Minimum Requirement Description
IPP.TR.01	Display	2 line or more, Monochrome display for viewing features like messages, directory
IPP.TR.02	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T
IPP.TR.03		Ethernet network through an RJ-45 interface
IPP.TR.04	Speaker Phone	Yes
IPP.TR.05	Headset	Wired, Cushion Padded Dual Ear- Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
IPP.TR.06	VoIP Protocol	SIP V2
IPP.TR.07	POE	IEEE 802.3af or better and AC Power Adapter (Option)
IPP.TR.08	Supported Protocols	SNMP, DHCP, DNS
IPP.TR.09	Codecs	G.711, G.722, G.729 including handset and speakerphone

IPP.TR.10	Speaker Phone	Full duplex speaker phone with echo cancellation
IPP.TR.11		Speaker on/off button, microphone mute
IPP.TR.12	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
IPP.TR.13	Phonebook/ Address book	Minimum 100 contacts
IPP.TR.14	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
IPP.TR.15	Clock	Time and Date on display
IPP.TR.16	Ringer	Selectable Ringer tone
IPP.TR.17	Directory Access	LDAP standard directory
IPP.TR.18	QoS	QoS mechanism through 802.1p/q

### 7.9.2 IP PBX (Call Control System)

S. No.	Nature of requirement	Minimum Requirement Description
PBX.TR.01	General	The IP telephony system should be a converged communication System with ability to run analog and IP on the same platform using same software load based on server and Gateway architecture
PBX.TR.02	Scalability	The single IP PBX system should be scalable to support up to 500 stations (any mix/percentage of Analog/IP) to achieve the future capacity
PBX.TR.03	General	The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted
PBX.TR.04	Architecture	The voice network architecture and call control functionality should be based on SIP
PBX.TR.05	Redundancy	The call control system should support redundancy with no single point of failure
PBX.TR.06	IP Support	The communication server and gateway should support IP V6 from day one so as to be future proof
PBX.TR.07	General	The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM
PBX.TR.08	General	Support for call-processing and call-control
PBX.TR.09	Protocols	Should support signaling standards/Protocols-SIP, MGCP, H.323, Q.Sig
PBX.TR.10	Codecs	Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC
PBX.TR.11	GUI	The System should have GUI support web based management console
PBX.TR.12		Security

S. No.	Nature of requirement	Minimum Requirement Description
PBX.TR.13	Security	The protection of signaling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS
PBX.TR.14	Security	System should support MLPP feature
PBX.TR.15	Security	Proposed system should support SRTP for media encryption and signaling encryption by TLS
PBX.TR.16	Security	Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory
PBX.TR.17	Security	The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
PBX.TR.18	General	Voice gateway to be provided with 1 PRI card with 2 port scalable to 3 PRI in future for PSTN (PRI) line termination.

### 7.9.3 Soft Phone

S. No.	Nature of requirement	Minimum Requirement Description
SP.TR.01	Soft Phone Client Features	Proposed soft phone client should be compatible with window based desktop & Android/ iPhone Mobile and should be provided with Desktop client
SP.TR.02		Should support Presence/Status, User-Choice Presence (Busy, be right back, Away, out to lunch / meeting etc.), Calendar Presence, coming from Microsoft Outlook calendar (if integrated).
SP.TR.03		Soft client shall be able to support one-to-one and multi-party messaging
SP.TR.04		It shall support ability to send Multimedia (Text, voice, video and photo) messages between users
SP.TR.05		It shall have ability to store messages centrally and be able to deliver them when users connect. Senders shall be able to send to offline receivers and messages shall be able to be delivered on demand. The centrally stored messages shall provide secure access through encryption between servers and endpoints.

S. No.	Nature of requirement	Minimum Requirement Description
		Also, data shall be available only through secured logins
SP.TR.06		Conversation persistency shall be maintained so that users can view and participate in active conversations from multiple messaging applications, until they leave the conversation
SP.TR.07		It shall support notification events for all new messages
SP.TR.08		It shall support user search for current and active conversations
SP.TR.09		It shall provide administrators to retrieve archived messages in future
SP.TR.10		It shall support synchronization with Microsoft Active Directory 2012
SP.TR.11		The UC Client shall be able to IM to group of Users defined by AD.
SP.TR.12		The UC Client shall provide Visual & Audio Tone Alerts on incoming Alerts
SP.TR.13		Shall provide the Presence indicator in IM buddy list and from email message
SP.TR.14		Shall provide Location Indicator: For Ex: Set your own locations like "Work", "Home", "Campus", "Sales Office" etc. so that next time the user signs-in from that office UC Client shall remember the location
SP.TR.15		Shall Provide Alert When Available: User shall be able to Set the client to notify him/her when a contact becomes available. User shall be notified the first time the user next becomes available. A message notification shall be given to alert the user that the user is available.
SP.TR.16		Spell Check shall be available in chat
SP.TR.17		Print Chat: The user shall have the ability to print a conversation with a right-click from a chat window with another user or by pressing CTRL + P. the user can also highlight a portion of the text to print it.
SP.TR.18		Group chat: UC Client shall allow users to define custom groups with support up to 100 groups. A group chat session shall support up to 500 users.

S. No.	Nature of requirement	Minimum Requirement Description
SP.TR.19		Persistent chat: Persistent chat rooms shall be supported to share ideas and information in a chat room and shall be active even after participants leave the room. When participants come back to the room, they can scroll back to read the messages that they missed. Persistent chat room shall have the capability to be password protected
SP.TR.20		Remove Group Chat Participants: The person who starts a group chat shall have the capability to remove group chat participants. Removed chat participants can be re-invited to the chat room at any time.
SP.TR.21		Screen share and Remote Desktop Sharing in Group Chat (1 : Many): Users shall have the capability to share screen with up to 5 people in group chat session using the IM-Only-desktop-sharing feature.
SP.TR.22		The UC Client shall support three Default Presence status and shall have support for multiple states.
SP.TR.23		Shall have the Provision to adjust presence status
SP.TR.24		Presence status shall be available for communication options
SP.TR.25		The user profile for IM and Presence is maintained in a common enterprise directory, e.g. existing active directory
SP.TR.26	Voice features	The Proposed client, apart from providing IM and presence functionality, shall be able to provide click to call functionality.
SP.TR.27		Shall support basic call control with a consistent client interface on PC, web interface, and mobile device.
SP.TR.28		Integration shall be able to provide: Initiate Call, terminate (Hang-Up Call), Hold, Transfer, Divert if Busy
SP.TR.29		Call Conferencing Capability
SP.TR.30		Shall be able to Initiate a conference call involving multiple participants.
SP.TR.31		Shall be able to Conference with participants using computer audio for voice
SP.TR.32		

S. No.	Nature of requirement	Minimum Requirement Description
SP.TR.33		Shall be able to Conference with participants using IP phone for voice
SP.TR.34		Ability to put a call on hold and resume the call from a different client associated with that user e.g. Hold the call from a PC and resume the call onto an iPad/Tablet or mobile phone.
SP.TR.35		The video calling capability to be part of the same client for IM and Presence.
SP.TR.36		Soft clients for Desktop, iOS or Android based tablets shall be able to participate in the video conferencing call.
SP.TR.37		The user shall be able to make point-to-point video calls without utilizing the MCU.

#### 7.9.4 IVR & ACD

S. No.	Nature of requirement	Minimum Requirement Description
ACD.TR.01	High Availability	Should support high availability with hot standby server that should provide seamless failover in case of main server failure. There should not be any downtime of Contact Center in case of single server failure in high availability case
ACD.TR.02	Routing	Should support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups
ACD.TR.03	Routing	ACD support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc.
ACD.TR.04	Routing	ACD should support call routing based on longest available agent, circular agent selection algorithms.
ACD.TR.05	Queuing	ACD should support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay.
ACD.TR.06	Chat	Agents should be able to chat with other Agents or supervisor and solution shall be provided with minimum 10 Agent licenses
ACD.TR.07	Status	Supervisor should be able to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop

S. No.	Nature of requirement	Minimum Requirement Description
ACD.TR.08	Queuing	Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.
ACD.TR.09	Active/Standby Mode	In future if required, the ACD should support active and standby server mode, where the server can be put in DC and DR. In case of Main server in the Data center fail the standby server in DR should take over seamlessly. ACD solution should support placing of Main and Stand by server in DC and DR respectively.
ACD.TR.10		Interactive Voice Response (IVR):
ACD.TR.11	DTMF	IVR should play welcome messages to callers Prompts to press and collect DTMF digits
ACD.TR.12	Self-Service	IVR should be able to integrate with backend database for self-service, as and when required.
ACD.TR.13	GUI	GUI based tool to be provided for designing the IVR and ACD call flow.
ACD.TR.14	Call Flows	IVR should support Voice XML for ASR, TTS, and DTMF call flows
ACD.TR.15	Read Capability	IVR should be able to Read data from HTTP and XML Pages
ACD.TR.16	Campaigns	IVR should be able to run outbound campaigns.
ACD.TR.17		Reporting:
ACD.TR.18	Performance Analysis	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc.
ACD.TR.19	Performance Analysis	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes
ACD.TR.20	Performance Analysis	Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.
ACD.TR.21	Performance Analysis	Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit or SQL stored procedures.
ACD.TR.22	Performance Analysis	Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF/RTF/XML/CSV.
ACD.TR.23		E-mail:
ACD.TR.24	Email	Administrator should be able to assign one or more email addresses to a single Queue.
ACD.TR.25	Email	Email routing support integration with Microsoft Exchange 2003 or Microsoft Exchange e2007 or 2010.
ACD.TR.26	Email	Agents should be able to automatically resume of e-mail processing on voice disconnect.

S. No.	Nature of requirement	Minimum Requirement Description
ACD.TR.27	Email	Agent should be able to save email draft response and resume at a later time.
ACD.TR.28	Email	Agent should be able to re-queue email.
ACD.TR.29	Email	Supervisor should be able to access real-time reporting for Agent E-Mail by mail volume

## 7.10 Variable Message Display (VMD) Board

S. No	Nature of requirement	Minimum Requirement
VMS-TR-01	Source of light	High intensity LEDs
VMS-TR-02	Colour	True Colour
VMS-TR-03	Brightness	>8000 cd/m <sup>2</sup>
VMS-TR-04	Luminance Class	L-3 as per EN 12966
VMS-TR-05	Contrast Ratio	R2-R3 as per EN 12966
VMS-TR-06	Beam Width	B-3 as per should be wide angle B6 or B7 or B4
VMS-TR-07	Viewing distance	>300 meters
VMS-TR-08	Display capability	Alpha-numeric, Pictorials, Graphical & video
VMS-TR-09	Pitch	10mm
VMS-TR-10	Display Front Panel	100% anti-glare
VMS-TR-11	Language	Multilingual (English/Hindi) and all fonts supported by windows
VMS-TR-12	Auto Dimming	Auto dimming adjusts to ambient light level
VMS-TR-13	In built Sensor	Photoelectric sensor
VMS-TR-14	Storage capacity	Minimum 100 GB
VMS-TR-15	Display Area	Display size of VMD should be 2.88m*1.92m
VMS-TR-16	Number of Lines	The number of lines and characters can be customized as per the requirement (Min 3 Lines & 10 Characters)
VMS-TR-17	Brightness & contrast	Controlled through software
VMS-TR-18	Display driving method	Direct current control driving circuit. Driver card of display applies Direct Current Technology
VMS-TR-19	Display Style	Stay on and flashing
VMS-TR-20	Connectivity	IP Based
VMS-TR-21	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
VMS-TR-22	Integration	With Smart City Operations Center and service providers for offering G2C and B2C services
VMS-TR-23	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment
VMS-TR-24	Battery	Internal Battery with different charging options (Solar/Mains)
VMS-TR-25	Power	Automatic on/off operation
VMS-TR-26	Casing	IP-55 rated for housing
VMS-TR-27	Operating conditions	0° to 55 °C

## 8. Technical Specifications Software

### 8.1 Integrated Command Control Centre

#### 8.1.1 Video wall management Software

S. No.	Nature of requirement	Minimum Specification Requirements
VWS.TR.01	General Requirements	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or based on the timer
VWS.TR.02	General Requirements	The software should enable the users to see the desktop of the graphics display wall remotely on any PC connected with the Display Controller over the Ethernet and change the size and position of the various windows being shown.
VWS.TR.03	General Requirements	The wall management software shall be having interoperability with Video management system.
VWS.TR.04	General Requirements	The wall management software may be centrally Server based or local controller based architecture.
VWS.TR.05	General Requirements	The software should enable various operators to access the display wall from the local keyboard and mouse of their workstation connected with the Display Controller on the Ethernet
VWS.TR.06	General Requirements	The software should copy the screen content of the PC / workstation connected on the Ethernet with the Display Controller to be shown on the Display wall in scalable and moveable windows in real time environment.
VWS.TR.07	General Requirements	The wall management software should enable Master System Integrators to integrate it with their Software.
VWS.TR.08	General Requirements	Key features of Wall management Software
VWS.TR.09		a. Central configuration database
VWS.TR.10	General Requirements	The Wall Control software shall perform health monitoring that allows timely detection of faults.
VWS.TR.11		a. Wall health
VWS.TR.12		b. Cube health
VWS.TR.13		c. Cube IP-address
VWS.TR.14		d. Brightness
VWS.TR.15	General Requirements	Wall Control Software shall allow commands on wall level or cube level or a selection of cubes :
VWS.TR.16		a. Switching the entire display wall on or off
VWS.TR.17		b. Fine-tune colour of each cube
VWS.TR.18	General Requirements	Log file functions

## 8.2 Data Centre - Software

### 8.2.1 Integrated Command & Control Centre (ICCC) Platform

S.NO.	Nature of Requirement	Functional Parameters/ Description		
ICCC.TR.01	Data Normalization capabilities	It is envisaged that the city shall implement multiple Smart City use cases over a period of time. The potential example Smart City use cases are Smart Traffic, Smart Parking, Smart Lighting, Energy Metering, Water Metering, CCTV, Public Transport, Public Wi-Fi and other integrations as per defined scope.		
ICCC.TR.02		The platform shall also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integration.		
ICCC.TR.03		The platform shall be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers.		
ICCC.TR.04		The platform shall support distributed deployment of functions (workflows & policies) across city's network and compute infrastructure with centralized management and control.		
ICCC.TR.05	GIS Map Support	System shall support Esri, Map Box, Open street etc. GIS and Map Servers		
ICCC.TR.06	Location engine	a)	Map services and geospatial coordinates: provides the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities.	
ICCC.TR.07		b)	Geospatial calculation: calculates distance between two or more locations on the map.	
ICCC.TR.08	Device engine	a)	Aggregation and abstraction of sensors: provides aggregation of sensors from diverse sensor cloud.	
ICCC.TR.09		b)	Normalization of sensor data: organizes sensor data and assigns attributes based on relations; raw data removed and passed to data engine.	
ICCC.TR.10	Data and Analytics engine	a)	Data archive and logging: stores data feeds from the device engine and external data sources.	
ICCC.TR.11		b)	Analytics: provides time-shifted or offline analytics on the archived data.	
ICCC.TR.12		c)	Reporting: delivers reports based on events triggered by device engine data and external notifications.	

S.NO.	Nature of Requirement	Functional Parameters/ Description
ICCC.TR.13	Developer Program tools	Sensor platform OEM shall provide online Developer Program tools that shall help City to produce new applications, and/or use solution APIs to enhance or manage existing solution free of cost.
ICCC.TR.14	Authentication, Authorization	System shall support standard Authentication, Authorization Perform.
ICCC.TR.15	Data plan Functionalities	Live data and visual feed from diverse sensors connected to the platform.
ICCC.TR.16	API Repository / API Guide	Normalized APIs shall be available for the listed domains (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example Lighting APIs: Vendor agnostic APIs to control Lighting functionality.
ICCC.TR.17		Platform OEM shall have published the normalized APIs in their website for the listed domains ((Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to allow sensor vendors and app developers to develop their connectors / adaptors to the platform.
ICCC.TR.18		Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future).
ICCC.TR.19	Platform upgrade and maintenance	The OEM shall be able to securely access the platform remotely for platform updates / upgrades and maintenance for the given duration.
ICCC.TR.20		Platform shall be able to be deployed on a public cloud for disaster recovery.
ICCC.TR.21	Platform functionality	API management and gateway: Provides secure API lifecycle, monitoring mechanism for available APIs.
ICCC.TR.22		User and subscription management: Provides different tier of user categorization, authentication, authorization, and services based on the subscriptions.
ICCC.TR.23		Application management: Provides role-based access view to applications.
ICCC.TR.24		The platform shall also be able to bring in other e-governance data as i-frames in the command and control centre dashboard.
ICCC.TR.25		All of these data shall be rendered / visualized on the command and control centre dashboard.
ICCC.TR.26	Integration capabilities	This platform is expected to integrate various urban services devices at the street layer so that urban services applications can be developed on top of this platform independent of the technology that is used in the devices.
ICCC.TR.27		Integrate devices using their APIs in to this platform. For example, if the City wants to deploy Smart

S.NO.	Nature of Requirement	Functional Parameters/ Description
		Parking solution, this platform shall have the ability and provision to write adaptors which interface with the parking sensors or management software of the parking sensors to collect parking events, data and alerts and notifications from the devices and their software managers.
ICCC.TR.28		The same logic and requirement applies to various other urban services devices like LED control nodes, water meters, energy meters, environmental sensors, waste bin sensors, device embedded in connected vehicles etc.
ICCC.TR.29		Enables the City and its partners to define a standard data model for each of the urban services domains (i.e. Parking, lighting, kiosks etc....).
ICCC.TR.30		Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices.
ICCC.TR.31		Provides urban services API(s) to develop Operations applications for each of the Urban Services domains. For example, the lighting operator of the City shall be able to develop a City Lighting management application based on the API(s) provided by the platform. This lighting application shall also have the ability to access data from other domains like environment based on the access control configured in the system.
ICCC.TR.32	Policies Events and	System shall allow policy creation to set of rules that control the behaviour of infrastructure items. Each policy shall a set of conditions that activate the behaviour it provides. System shall allow Default, Time-based, Event-based and Manual override policies creation. For example, an operator might enforce a "no parking zone" policy manually to facilitate road repairs.
ICCC.TR.33		System shall provision to define a set of conditions that can be used to trigger an event-based policy
ICCC.TR.34		System shall generate Notification, Alert and Alarm messages that shall be visible within the Dashboard/GIS Platform and the Enforcement Officer Mobile App if required.
ICCC.TR.35	Notifications, Alerts and Alarms and	All system messages (notifications, alerts and alarms) shall always be visible from the Notifications view, which provides controls that operator can use to sort and filter the messages that it displays.
ICCC.TR.36		Systems shall deliver message to a set of subscribers. The Notification service shall support min. two types

S.NO.	Nature of Requirement	Functional Parameters/ Description
		of notification methods – Email notification and Short Messaging Service (SMS) notification.
ICCC.TR.37	Users and roles	Users access and perform various tasks, such as adding new locations, configuring new devices, managing adapters, and so on. However, not all users can perform all tasks. Each user shall be associated with one or more roles and each role is assigned a certain set of permissions.
ICCC.TR.38		These roles and permissions define the tasks that a user can perform. Additionally, system shall assign one or more locations to each role so that the user can perform tasks at the assigned locations only.
ICCC.TR.39		Roles and permissions define the tasks that a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. Each user shall be associated with one or more roles and each role has an assigned set of permissions.
ICCC.TR.40		The platform shall allow different roles to be created and assign those roles to different access control policies.
ICCC.TR.41		System shall support LDAP to be used as an additional data store for user management and authentication.
ICCC.TR.42	Service Catalog Management	The Service catalog management module shall allow to categorize the externalized and non-externalized services into logical groups by creating the service catalogs. In addition, system shall allow manage the service catalog by adding, modifying or deleting the catalog details.
ICCC.TR.43	Reports	The platform shall have capability to provide access to real time data and historical data from various connected devices for reporting and analytics.
ICCC.TR.44		System shall allow dashboard to generate reports and have provision to add reports in favourites list.
ICCC.TR.45	Data Security	The access to data shall be highly secure and efficient.
ICCC.TR.46		Access to the platform API(s) shall be secured using API keys.
ICCC.TR.47		Software shall support security standards: OAuth 2.0, HTTPS over SSL or equivalent security standards help protect the data across all domains.
ICCC.TR.48	Global Market Presence & Support System	Smart city suppliers shall be adaptable to the emerging needs of cities. Suppliers shall develop offerings that meet the growing interest in urban Internet of Things (IoT) applications, big data solutions, and the transformation in city approaches to energy policy, urban mobility, and city resilience.
ICCC.TR.49		Smart City Platform/Software provider shall be global Member of Smart Cities Council & Navigant Research Report for Smart Cities Suppliers.

S.NO.	Nature of Requirement	Functional Parameters/ Description
ICCC.TR.50		ICCC OEM shall have registered office in India at least from last 05 Years and shall have software development centre in India. Shall have Quality Management System ISO 9001 OR Environmental Management System ISO 14001 Quality Certifications.
ICCC.TR.51		Command & Control Centre shall provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
ICCC.TR.52	Standard Operating Procedure	Standard Operating Procedures shall be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an Operations.
ICCC.TR.53		The users shall be able to edit the SOP, including adding, editing, or deleting the activities.
ICCC.TR.54		The users shall be able to also add comments to or stop the SOP (prior to completion).
ICCC.TR.55		There shall be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
ICCC.TR.56		The SOP Tool shall have capability to define the following activity types:
ICCC.TR.57		Manual Activity - An activity that is done manually by the owner and provide details in the description field.
ICCC.TR.58		Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.
ICCC.TR.59		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
ICCC.TR.60		Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
ICCC.TR.61		SOP Activity - An activity that launches another standard operating procedure.
ICCC.TR.62	Analytics Engine	Analytics Engine shall be an artificial intelligence-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The machine learning capabilities aid in automating policies that result in better asset and infrastructure management.
ICCC.TR.63		The solution shall be flexible to integrate with other city and government software applications.

S.NO.	Nature of Requirement	Functional Parameters/ Description
ICCC.TR.64		<p>Analytics Engine module shall have below intelligence capabilities;</p> <ul style="list-style-type: none"> <li>a) Advanced Predictive Analytics shall be part of the solution.</li> <li>b) The solution shall be flexible to integrate with other city and government software applications</li> <li>c) The solution shall be able to predict insights consuming data from city infrastructure viz., Traffic, Parking, Lighting etc.</li> <li>d) The solution shall have predictions with measurable accuracy of at least &gt; 70%</li> <li>e) The solution shall be able to predict and integrate with Smart City solutions helping in driving Operational policies creation.</li> <li>f) The solution shall be robust, secure and scalable.</li> <li>g) The solution shall have a visualization platform to view historic analytics</li> </ul>
ICCC.TR.65		<p>The application shall enable the customers to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level, when you work with the application, system do the following tasks:</p> <ul style="list-style-type: none"> <li>a) Connect to a variety of data sources</li> <li>b) Analyze the result set</li> <li>c) Visualize the results</li> <li>d) Predict outcomes</li> </ul>
ICCC.TR.66		<p>Analytics Engine shall support multiple Data Sources. Min below standard data sources shall be supported - CSV, TSV, MS Excel , NOSQL, RDBMS</p>
ICCC.TR.67		<p>Analytics Engine shall provide analysis of data from a selected data source(s).</p> <p>Analysis enables to define arithmetic and aggregation Operations that result in the desired output.</p> <p>Analytics engine shall provide capability to check analysis with multiple predictive algorithms.</p>

S.NO.	Nature of Requirement	Functional Parameters/ Description
ICCC.TR.68	Analytics Engine Visualizations	<p>Analytics Engine shall provide visualizations dashboard.</p> <p>In the visualization workspace it shall allow to change visual attributes of a graph.</p> <p>User shall not be allowed to alter the graph/visualization definition.</p> <p>In the visualizations workspace, user shall able to do the following Operations:</p> <ul style="list-style-type: none"> <li>a) Change the graph/visualization type</li> <li>b) Print the graph</li> <li>c) Export the graph</li> <li>d) Narrow down on the value ranges</li> <li>e) Toggle the axis labels</li> <li>f) Integrate with other 3<sup>rd</sup> party applications seamlessly</li> </ul>
ICCC.TR.69	Export Formats	<p>System shall allow export the analysis into min following formats:</p> <ul style="list-style-type: none"> <li>a) XML/JSON</li> <li>b) Excel</li> <li>c) PDF</li> <li>d) CSV</li> </ul>
ICCC.TR.70	Video Display and integration capabilities	<ul style="list-style-type: none"> <li>a) Integrates with existing cameras and new cameras. Shall support multiple video sources from multiple locations. Platform shall have no limitation in displaying the number of CCTV video sources.</li> <li>b) Integrate and assess inputs from different sources such as CCTV, Video Analytics, and sensors further to assist with actionable intelligence.</li> <li>c) Display module shall have capability to control multi-screened display wall in sync with operator console.</li> <li>d) Smart City Operations Centre shall support 20 to 30 camera feeds in display.</li> </ul>
ICCC.TR.71	Technical support centre	ICCC OEM shall have 24x7x365 technical assistance support centre (TASC) in India. TASC shall provide online website and phone number to register service request, service request can be raise by partner and customer.
ICCC.TR.72	CCC Operations	<ul style="list-style-type: none"> <li>a) The solution shall be implemented and compliant to industry open standard commercial-off-the-shelf (COTS) applications that are customizable.</li> <li>b) The solution shall integrate with GIS and map information and be able to dynamically update</li> </ul>

S.NO.	Nature of Requirement	Functional Parameters/ Description
		<p>information on the GIS maps to show status of resources.</p> <ul style="list-style-type: none"> <li>c) The solution shall also provide an integrated user interface for all the smart elements implemented.</li> <li>d) The solution shall provide operators and managers with a management dashboard that provides a real time status and is automatically updated when certain actions, incidents and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. The above attributes shall be colour coded.</li> <li>e) The solution shall provide the "day to day Operations", "Common Operating Picture" and situational awareness to the centre and participating agencies during these modes of Operations.</li> <li>f) It shall improve scalability for large and geographically distributed environments.</li> <li>g) It shall provide complete view of sensors, facilities, e-governance/ERP, video streams and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.</li> <li>h) It shall provide a uniform, coherent, user-friendly and standardized interface.</li> <li>i) It shall provide possibility to connect to workstations and accessible via web browser.</li> <li>j) The dashboard content and layout shall be configurable and information displayed on these dashboards shall be filtered by the role of the person viewing dashboard.</li> <li>k) The solution shall allow creation of hierarchy of incidents and be able to present the same in the form of a tree structure for analysis purposes.</li> <li>l) The solution shall be available via a VPN as a web-based interface or a thin-client interface.</li> <li>m) It shall be possible to combine the different views onto a single screen or a multi-monitor workstation.</li> <li>n) The solution shall maintain a comprehensive and easy to understand audit trail of read and write actions performed on the system.</li> </ul>

S.NO.	Nature of Requirement	Functional Parameters/ Description
		<ul style="list-style-type: none"> <li>o) The solution shall provide ability to extract data in desired formats for publishing and interfacing purposes.</li> <li>p) The solution shall provide ability to attach documents and other artefacts to incidents and other entities.</li> <li>q) The solution is required to issue, log, track, manage and report on all activities underway during these modes of Operations: <ul style="list-style-type: none"> <li>· anticipation of incident</li> <li>· incident or crisis</li> <li>· recovery</li> <li>· incident simulation</li> </ul> </li> </ul>
ICCC.TR.73	Analytics and Telemetry monitoring	<ul style="list-style-type: none"> <li>a) Analytics appliance must monitor and display each and every process running on the server (Physical / VM form factor). Appliance must also display the process ID, Process owner, Process mapping etc.</li> <li>b) Analytics appliance must uses machine learning algorithm to build application insight and its interdependency to create real time application dependency mapping for the desired time range.</li> <li>c) Analytics appliance should be capable of simulating what if scenario with existing policy on past traffic or new policy on current / old traffic and validate the result before applying the policy on the production network.</li> <li>d) Analytics appliance should collect data from each server using sensor / agent.</li> <li>e) Analytics appliance agent should have bidirectional authentication with the analytics appliance to avoid security spoofing.</li> <li>f) Analytics appliance must manage, monitor and upgrade the agent deployed onto the server.</li> <li>g) Analytics appliance agent should support and deployed on the following windows and Linux OS in bare metal or VM form factor:</li> <li>h) A] Linux - RHEs Release 5.3 and later, RHEs release 6.x, Cent OS Release 5.11 and later, Cent OS release 6.x, Ubuntu Release 12.04, 14.04, 14.10</li> </ul>

S.NO.	Nature of Requirement	Functional Parameters/ Description
		<ul style="list-style-type: none"> <li>i) B] Microsoft Windows Server - MWS 2008, 2008 R2, 2012 and 2012 R2 Standard, Enterprise, Essentials and Data Centre Editions</li> <li>j) Analytics appliance should also support hardware sensor running on the network switches for gathering buffer utilization, burst detection, network latency, packet drops etc. details.</li> <li>k) Analytics appliance must have its own WebGui.</li> <li>l) Analytics appliance must support Open North bound REST API as well as KAFKA based push events.</li> <li>m) Analytics appliance monitor compliance and compliance deviations and report back in minute in case of any non - compliance.</li> <li>n) Analytics appliance must recommend and validate/simulate whitelist policy for each application.</li> <li>o) Analytics appliance should support policy impact analysis and test policy / white list policy before enforcing it to the production environment in DC.</li> <li>p) Analytics appliance should provide contextual search capability with actionable insight for faster troubleshooting and anomaly detection.</li> <li>q) Analytics appliance must collect telemetry information from every packet in the data centre without sampling as well as it must support long term data (flow information) retention.</li> <li>r) Analytics appliance must support role based authentication (RBAC) for Web GUI and REST API.</li> <li>s) Analytics appliance should analyze each and every flow in different dimension i.e. location, time of transaction, network and application latency, source and destination ports and IP, Session duration etc. to find out application anomaly</li> <li>t) Analytics appliance should be capable of exporting the policy recommendation in to JSON, XML and YAML</li> <li>u) Analytics appliance should be capable of supporting 5,000 end points (i.e. VMs, Servers, Switches etc.) and scalable to 10,000 end points with license upgrade only.</li> <li>v) Analytics appliance should be horizontal scalable.</li> </ul>

S.NO.	Nature of Requirement	Functional Parameters/ Description
ICCC.TR.74	API & Interface Security	<p>a) The access to data shall be highly secure and efficient.</p> <p>b) Access to the platform API(s) shall be secured using API keys.</p> <p>c) Software shall support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.</p> <p>d) Shall support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.</p>

#### 8.2.2 Enterprise Content Management System / Document Management System

S. No.	Indicative Requirement Description
CMS.TR.001	<p>Facility to scan and upload</p> <ul style="list-style-type: none"> <li>• Paper documents</li> <li>• Photos</li> <li>• Email communication</li> <li>• Any other document</li> </ul>
CMS.TR.002	Documents in electronic soft form (pdf, txt, xls, doc, ppt, picture files, TIFF, JPEG, GIF, even Zip Files) System generated documents
CMS.TR.003	Ability to share documents scanned across several offices / departments.
CMS.TR.004	The proposed system shall have Out of the Box capability of Digital Asset management to manage rich media content files.
CMS.TR.005	Automatically create multiple formats of a corporate image or video and create additional formats with various aspect ratio on ingestion
CMS.TR.006	Support multiple definitions of sets of renditions to be created for different classes of assets
CMS.TR.007	System shall have support for management of image formats such as JPG, GIF, PNG, TIFF, PSD, and BMP; as well as output formats such as JPG, GIF, PNG, and PSD.
CMS.TR.008	System shall have support for video formats such as Flash, Real, Windows Media Format, QuickTime, and others. Image and Video metadata is extracted and associated with the content item as object metadata.
CMS.TR.009	Ability to check the quality of the scanned image and make corrections/adjustments to improve the quality of the scanned image.
CMS.TR.010	The ECM shall support temporarily storing the scanned images locally before uploading to the central server.
CMS.TR.011	Ability to support quick scanning and indexing of bulk documents. Scanning through browser plug-in.
CMS.TR.012	Ability to support automatic cropping / masking of whole/any part of the document. This ability should be user defined and also document wise.

S. No.	Indicative Requirement Description
CMS.TR.013	It shall be possible to scan and upload documents including pictures and images. Such document may be uploaded directly from third party premises over the web or from the office.
CMS.TR.014	Ability to support Web based scanning
CMS.TR.015	It shall be possible to set up and track both mandatory and non-mandatory documents.
CMS.TR.016	Document types need to be pre-defined as a product / type of service / transaction type / workflow etc.
CMS.TR.017	Confirm that the content was delivered and viewed as a proof of compliance with security policies
CMS.TR.018	Grant access to documents offline for a specified period of time while maintaining audit capabilities.
CMS.TR.019	The system shall have a native iOS and Android based mobile/tablet app for easy access of the information (document) while users are on the move.
CMS.TR.020	Workflow for routing and tracking of documents, messages and Forms
CMS.TR.021	Create Ad-hoc or predefined routes for automatic document routing on sequential / parallel routes. This must be offered as a base and standard product
CMS.TR.022	Facility of associating a note-sheet with the file enabling users to comment and review.
CMS.TR.023	Facility of attaching documents and folders in work items
CMS.TR.024	Facility to act upon, forward, return or complete Work-items
CMS.TR.025	Support for referring Work-items to other users outside the pre-defined route
CMS.TR.026	Time -based/ Event -based reminders
CMS.TR.027	Provision of putting shared and secured notes for collaborative working on Work items
CMS.TR.028	Ability to support typical document imaging annotations which include:
CMS.TR.029	<ul style="list-style-type: none"> <li>• Highlighting images and text in various colours to emphasize words or sections</li> </ul>
CMS.TR.030	<ul style="list-style-type: none"> <li>• Redacting (blacking-out or whiting-out) images and text to preserve confidentiality</li> </ul>
CMS.TR.031	<ul style="list-style-type: none"> <li>• Stamping images with words such as FAXED or CONFIDENTIAL, or with signatures denoting approval or denial</li> </ul>
CMS.TR.032	<ul style="list-style-type: none"> <li>• Attaching sticky notes that contain additional comments</li> </ul>
CMS.TR.033	An imaging system 's security should control who can view
CMS.TR.034	<ul style="list-style-type: none"> <li>• Annotations such as highlighting, stamps or sticky notes, and who can see through redaction. All annotations should be overlaid and not change the actual image.</li> <li>• Ability to support Printing, faxing and e-mailing documents</li> </ul>
CMS.TR.035	System shall provide web-based administration tool and provide a single point of access for managing and administering all repositories, servers, users and groups regardless of their location across the enterprise
CMS.TR.036	The system shall allow content syndication service via xml based feeds, email alerts etc.
CMS.TR.037	The system shall support versioning of contents, user should be able to access previous and next versions
CMS.TR.038	Shall support storage of complete and multiple versions of content

S. No.	Indicative Requirement Description
CMS.TR.039	Shall have major & minor release for draft & final release version of the document
CMS.TR.040	Shall support the JSR 170, Java APIs/REST APIs/Web Service APIs that make content assets available to the application layer services or other Content Management (CM) solutions.
CMS.TR.041	Shall support for storage of any type of contents such as JPG, TIFF, PDF, MS office files, audio, video, auto cad files etc.
CMS.TR.042	The product shall support single metadata store for modules such as Document Management, Web Content Management, Records Management and Digital Asset Management
CMS.TR.043	System should provide library services such as core content services, workflows, archiving, folders, content publishing, records management and security features.
CMS.TR.044	Ability to support a single Security model for the content repository that is used to manage documents, records as well as web content.
CMS.TR.045	Shall have out of box support for standards like BPM/BPEL to address complex workflow requirements
CMS.TR.046	System shall support for auditing for usage of content through audit trails
CMS.TR.047	System shall provide support for scheduling indexing
CMS.TR.048	Provides ability for administrators to archive and backup content
CMS.TR.049	Shall support for both centralized & distributed architecture
CMS.TR.050	Shall support for content cache for remote client
CMS.TR.051	Shall have policy-based, pluggable framework for reliability and secure access.
CMS.TR.052	Shall have a comprehensive access control functions, depending on the user role & access levels
CMS.TR.053	Shall support simple as well as complex workflows along with escalation routing and monitoring policy as defined by user
CMS.TR.054	The proposed system shall be able to classify any piece of content as a record
CMS.TR.055	Support for creation, declaration, classification, retention and destruction of business records.
CMS.TR.056	System shall provide audit trails and certificate of destruction.
CMS.TR.057	System shall provide the ability to freeze the records.
CMS.TR.058	Product shall provide records managers with a single view into all retention schedules, disposition actions, and audit histories, facilitating the process of identifying and declaring records.
CMS.TR.059	System shall allow for management of external content.
CMS.TR.060	System shall support adapters to external repositories for managing records, such as file systems, content repositories and e-mail archives
CMS.TR.061	Product shall provide generic adapters that can be configured for integration with other applications and repositories.
CMS.TR.062	It shall have out of box components and integration options with Portal
CMS.TR.063	The system shall provide ability to leverage multiple display templates for a content item
CMS.TR.064	System shall support in-context web content contribution, preview, updates and approvals.
CMS.TR.065	System shall provide support for multi-site management

S. No.	Indicative Requirement Description
CMS.TR.066	The system shall provide spell-checking functionality. The language of the dictionary must be able to be changed for content authors producing content in other languages.
CMS.TR.067	The system shall provide the ability to upload and associate media items to content items from within the content item authoring interface.
CMS.TR.068	The system shall provide the ability to preview content as it shall appear on pages where it is added in production prior to it being published
CMS.TR.069	Digital Certificate Services: The system should automatically enable/disable the Digital Signature Certificates (DSCs) of employees depending on the current status of each employee namely, fresh appointment / transfer / leave/ training / retirement etc. The system should accordingly enable DSC only for an "active" employee. Procurement of digital certificates for the users of the BMC shall be the responsibility of the client.
CMS.TR.070	MAILING AND MESSAGING SERVICES: This would be used for sending the alerts as mail and SMS message to the registered users of the application and shall be used for messaging and calendaring services. The Mail and SMS Server should provide a highly available, scalable and reliable platform for delivering secure communication services. It would be required to cluster this Server to ensure high availability and reliability. This server shall also act as Messaging Server. It should provide with extensive security features ensuring the privacy of users and the integrity of communication through user authentication, session encryption, and content filtering to help prevent spam and viruses, and mechanisms to monitor and enable regulatory compliance. It should support standard SMTP, IMAP and POP3 services. The Messaging system should provide a secure messaging and collaboration - email solution with standard features like calendaring, contacts and tasks, Archiving, Directory and LDAP address book, web based access to emails and support for data storage. Other features to be supported include - per-user filtering policies, user management, mailing list manager and synchronization with MS Outlook / Lotus Notes/ equivalent. Approximate size of mailbox for registered user should be 300MB.
CMS.TR.071	PAYMENT GATEWAY: The application would provide the online payment services through integration with the payment gateways. The solution shall support card payments using all the popular debit and credit cards (Visa, Master card etc.) and Direct Debit. For online payments, Secure Socket Layer (SSL) shall be used for supporting & securing the transactions taking place through the payment gateway. As Commercial transaction over internet is prone to Identity Theft and can cause financial loss to department and citizens, the solution would incorporate PCI DSS ver. 1.1 standards. Currently BMC has set up a payment gateway with Axis bank.

### 8.2.3 EMS and Network Monitoring System

S. No.	Nature of requirement	Minimum Requirement Description
EMS.TR.01	General	Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise

S. No.	Nature of requirement	Minimum Requirement Description
		resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure present in the enterprise
EMS.TR.02	General	The Service Management solution to be used for incident and problem management, Inventory& Asset management, Service Request Management, Self Service, Service level management should be built to leverage the same common Configuration Management Database (CMDB) with a unified architecture
EMS.TR.03	General	The service automation solution should provide configuration management and compliance assurance across servers, networks and applications
EMS.TR.04	General	Solution should provide for future scalability of the whole system without major architectural changes
EMS.TR.05	General	Solution should be distributed, and scalable and open to third party integration
EMS.TR.06	General	The solution should be able to monitor all the IT assets for the organization across all the location spread across including servers, network, routers, switches etc.
EMS.TR.07	General	The agent and agentless monitor should be able to collect & manage event/ fault, performance and capacity data and should not require separate collectors
EMS.TR.08	General	The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events
EMS.TR.09	Technical	The solution should have the capability to identify probable root cause using a variety of filtering and statistical correlation methods to determine their relevance to the issue being researched
EMS.TR.10	Technical	The solution should be able to generate dynamic performance baselines and continuously update and refine these normal operational bands by automatically adapting to the changes in enterprise infrastructure
EMS.TR.11	Technical	The solution should have the capability to perform automated dynamic threshold management

S. No.	Nature of requirement	Minimum Requirement Description
EMS.TR.12	Technical	The solution should carry out automated probable cause analysis by picking up feeds from every infrastructure component being monitored and automating the correlation of these alarms/ events to point out the probable cause of an infrastructure error
EMS.TR.13	General	Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation
EMS.TR.14	General	Should be configurable to suppress events for key systems/ devices that are down for routine maintenance or planned outage
EMS.TR.15	General	The solution should provide the mechanism for creation of knowledgebase and provision the same to the end users with the ability to search for known errors from the knowledge base
EMS.TR.16	General	The solution should provide network, server, application and database performance information and alarms and should be able to show it in a single console and provide a reporting interface for all network and system components
EMS.TR.17	General	The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors
EMS.TR.18	Technical	Should be able to monitor & manage distributed & heterogeneous systems (both 32 bit & 64 Bit) - Windows, UNIX & LINUX, including various market leading virtual platforms like VMware, Microsoft HyperV etc.
EMS.TR.19	General	Database Monitoring: The solution should be able to monitor all the market leading database solution providers
EMS.TR.20	General	The Database monitoring should seamlessly integrate with the same EMS dashboard/ Portal and provide integration with the central event console
EMS.TR.21	General	The tool should provide the organization the ability to easily collect and analyse specific information of applications & databases

S. No.	Nature of requirement	Minimum Requirement Description
EMS.TR.22	Technical	Servers: Should be able to monitor the server instances, database and instance status, initialization parameters, CPU usage, and SQL tracing
EMS.TR.23	Technical	Application monitoring parameters:
EMS.TR.24	Technical	Database Monitoring Attributes but not limited to:
EMS.TR.25	Technical	User Connections(#)
EMS.TR.26	Technical	Transaction Count
EMS.TR.27	Technical	Log Space Available
EMS.TR.28	Technical	Deadlocks/ sec
EMS.TR.29	Technical	Database Free Space (%)
EMS.TR.30	Technical	Database Used Space (MB)
EMS.TR.31	Technical	Disk Reads (per sec)
EMS.TR.32	Technical	Disk Writes (per sec)
EMS.TR.33	Technical	Cache hit ratio
EMS.TR.34	Technical	Lock Memory
EMS.TR.35	Technical	Average Wait Time(per table)
EMS.TR.36	Technical	Buffer Cache Hit Ratio (%)
EMS.TR.37	Technical	Commits (per sec)
EMS.TR.38	Technical	Memory Used (MB)
EMS.TR.39	Technical	Percent Memory Used (%)
EMS.TR.40	Technical	Availability (%)
EMS.TR.41	Technical	Commits (per sec)
EMS.TR.42	Technical	Percent Memory Used (%)
EMS.TR.43	Technical	Buffer Cache Hit Ratio (%)
EMS.TR.44	Technical	Active Instances (#)
EMS.TR.45	Technical	Provide details of various application frameworks like but not limited to the following: Portal, Java Application Server, Microsoft .NET, etc.
EMS.TR.46	Technical	Web Server Monitors but not limited to:
EMS.TR.47	Technical	Post Requests (per sec)
EMS.TR.48	Technical	Get Requests (per sec)

S. No.	Nature of requirement	Minimum Requirement Description
EMS.TR.49	Technical	Errors (per sec)
EMS.TR.50	Technical	Client Side Errors (per sec)
EMS.TR.51	Technical	Server Side Errors (per sec)
EMS.TR.52	Technical	Percent Busy Connections (%)
EMS.TR.53	Technical	Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different parameters like CPU utilization, disk space, response times , resolution times (e.g. incident closed on 2 hours) performance and custom parameters of an enterprise etc.
EMS.TR.54	Technical	The solution should have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance
EMS.TR.55	General	The solution should manage service levels for delivery and support of business services
EMS.TR.56	General	The solution should have real-time visualization of service level targets, agreement compliance data, penalties and rewards
EMS.TR.57	General	Should support compliance and cost trending to assist in identifying areas for process and operational improvements
EMS.TR.58	General	Provide users (based on role and access defined for that user) to drill down to specific report/ data on a need basis
EMS.TR.59	General	Ability to create custom KPI metrics and scorecard/ compliance reports that are updated automatically
EMS.TR.60	General	Single dashboard provides the as-is scenario by consolidating the data across the organization
EMS.TR.61	General	Should support top down dashboards with drill down capabilities into detailed information
EMS.TR.62	General	Should support comprehensive and configuration-level roll-back for changes
EMS.TR.63	General	Policy-based, Cross-Platform patch support across Windows, Linux, and Unix

S. No.	Nature of requirement	Minimum Requirement Description
EMS.TR.64	General	Support Granular and environment aware configuration policies and deployment
EMS.TR.65	General	Should support cross-platform and reusable packaging with built-in rollback support
EMS.TR.66	General	Should support Configuration-level Control of Tasks, Objects, and Policies
EMS.TR.67	General	Should have ability to monitor the parameters and confirm compliance to security policies
EMS.TR.68	General	Should have audit capabilities that compare the server status to policies defined in real time/ scheduled basis
EMS.TR.69	General	It should provide data filtration based upon user measurements (i.e., specific users, pages, requests, or transactions) to observe and analyse and track user activity at the individual or group level
EMS.TR.70	General	It should automatically trends and provides dynamic performance baselines for applications and services
EMS.TR.71	General	It should proactively identify errors affecting end-users, instead of waiting for a call from an employee or an incident being raised
EMS.TR.72	General	It should provide comprehensive view of application performance from the end-user perspective; it should distinguish between broad and targeted slow-downs, allowing drill-down into
EMS.TR.73	General	Details
EMS.TR.74	General	It should automatically collect, organize, and analyse all end-user experience data and present all relevant data in a meaningful and easy to-consume format like PDF, CSV, Excel etc) to enable rapid problem detection and isolation
EMS.TR.75	General	The solution should look at a single user and track their activity across an application. Shows where problems are encountered, or why a particular instance of a page took a long time to load.
EMS.TR.76	General	It should use real end user performance as one of the feed for more accurate root cause analysis and automated repair of business service performance issues

#### 8.2.4 Identity Access Management Software (IAM)

S. No.	Minimum Requirement Description
IAM.TR.001	System shall be able to identify, authorize and authenticate the user and would allow access to the applications and database based on the user identity.
IAM.TR.002	Identity and access management system would be able to identify the rights available with the user in terms of viewing, addition, deletion, modification of the data and generation of various reports through MIS.
IAM.TR.003	It would be possible to revoke the rights of users
IAM.TR.004	The functionality for user maintenance such as creating users, creating teams, enabling and disabling users, deleting Users, assigning security roles to users, identifying managers for Users and assigning users to teams shall be considered
IAM.TR.005	Single sign on and prioritizing key and normal users to be included as a part of IMS
IAM.TR.006	Maintenance of the VPN users

#### 8.2.5 Directory Services

S. No.	Minimum Requirement Description
DS.TR.001	Directory services would have a provision to create, update and modify the LDAP directory
DS.TR.002	It would have a provision to integrate with the Identity and access management
DS.TR.003	It would be used to define the roles and permission of different kinds of users in the system
DS.TR.004	Directory services would have proper integrations with DNS, DHCP, Email and other infrastructure components and services.

#### 8.2.6 Backup Software

S. No.	Minimum Specification Requirements
BKS.TR.01	The offered Software must support GUI with centralized management / Single interface for management of all backup activities.
BKS.TR.02	Backup software should be an image level backup software supporting popular hypervisors like VMware and Hyper-V Virtual Environments. Provide Block level Incremental and Differential Backup and support Incremental and Differential Imaging.
BKS.TR.03	Backup software should be totally agentless but should support application aware backups for MS SQL, Oracle, and Exchange with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads.
BKS.TR.04	Backup software should store a backup recovery point as a single file.
BKS.TR.05	Backup software should have integrated data de-duplication engine with multi-vendor storage support to save de-duplication data.
BKS.TR.06	The software should support varieties of backup mechanisms like Full, Incremental, and Differential etc. at different frequencies i.e. yearly, monthly, weekly, daily, hourly etc. as per defined policy. It should also have calendar-based backup scheduling. The restoration should also be supported accordingly.

S. No.	Minimum Specification Requirements
BKS.TR.07	Backup software should integrate with Disk Backup target device which supports hardware/software data deduplication capabilities.
BKS.TR.08	The proposed backup software should provide recovery from physical servers to Virtual and image level recovery.
BKS.TR.09	Backup software should provide best RTOs and RPOs through booting of Virtual Machines directly from the Backup to reduce the downtime.
BKS.TR.10	The offered software license must be proposed as per solution for seamless access.
BKS.TR.11	Five year premium level 24x7 Annual Technical Support (ATS) for software license.

### 8.2.7 Antivirus Solutions

S. No.	Minimum Requirement Description
AVS.TR.001	Anti-virus shall have auto update feature, it shall be able to push signature from the centralized server to all the clients Or workstations
AVS.TR.002	Bidder shall ensure that the scan logs are made available for review.
AVS.TR.003	The solution must support mass mailing virus detection.
AVS.TR.004	The solution must support mail attachment virus detection.
AVS.TR.005	The solution must support Malformed Mail format detection.
AVS.TR.006	The solution must have a built in Safe Stamp feature to have a sign of a secure email. The email scanning time stamp shows whether the sender's antivirus database is not up to date or not.
AVS.TR.007	The solution must have its own Updated Recommended Virus Extensions.
AVS.TR.008	The solution must support Heuristics-based mail header detection for Spam.
AVS.TR.009	The solution must support Heuristics-based scanning of the mail body for Spam.
AVS.TR.010	The solution must support administrator defined Anti-Spam exception list (approved list).
AVS.TR.011	The solution must support administrator to define list of known spammers.
AVS.TR.012	The solution shall be able to detect Spam in form of categories like general, commercial email, Get rich quick, pornography etc.
AVS.TR.013	The solution shall be able to take action based on the category in which Spam is detected.
AVS.TR.014	The solution must be able to take different action based on the different sensitivity level of Spam detection.
AVS.TR.015	The solution must provide alerts based on action taken on the Spam mail.
AVS.TR.016	The solution must support Encrypted MailDetection.
AVS.TR.017	The solution must support Password Protect Zip Detection.
AVS.TR.018	The solution must have a Secure SSL Web Management Console.
AVS.TR.019	The solution must be able to prevent System Denial of Service ('Do's') Attack.
AVS.TR.020	Bidder shall propose the required hardware for the entire solution
AVS.TR.021	Bidder shall provide requisite licenses for all the software required for the Anti-virus and Antispam Solution.
AVS.TR.022	Solution should provide protection against Back Doors and Trojan Horses
AVS.TR.023	Solution should provide real time fraud and risk management including but not limited to behavioural analysis, key loggers, Trojans and should allow

S. No.	Minimum Requirement Description
	monitoring on transactions and raise alerts in case of suspicious activities as defined by the security policy of organization.

### 8.2.8 Automation and Orchestration Solution

S. No.	Minimum Requirement Description
SVAO.STR.001	Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS/ SaaS services for Smart City applications so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM and movement within and across DC & DR.
SVAO.STR.002	Solution should be built using programmable & policy defined infrastructure components which should be independent of underlying hardware components and use standard x86 servers, storage, switches from any OEM make and model.
SVAO.STR.003	Solution must provide auto scale so that in case of increase in load/connections/users. Additional VMs should be automatically created with all network, security and load balancing policies. Integration required from cloud portal, orchestration, virtualization, virtual network, security and load balancing should be done to achieve this functionality
SVAO.STR.004	Solution must provide cloud operations layer integrated with automation layer which provides proactive monitoring, alerts, management, and capacity planning and performance management.
SVAO.STR.005	Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.
SVAO.STR.006	Solution should provide monitoring and management of complete virtualized infrastructure with prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements

### 8.2.9 Compute Virtualization Solution (Compute)

S. No.	Minimum Requirement Description
SV.TR.001	Sits directly on the bare metal server hardware with no dependence on a general-purpose OS for greater reliability & security and should be Leaders/Challengers in the Gartner's Magic Quadrant for at least last 2 years in a row.
SV.TR.002	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc.
SV.TR.003	Live Virtual Machine migration between different generations of CPUs in the same cluster without the need for shared storage option and long distances from one site to another (up to 150 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.
SV.TR.004	Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS

S. No.	Minimum Requirement Description
SV.TR.005	<ul style="list-style-type: none"> <li>Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs</li> <li>Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software.</li> </ul>
SV.TR.006	Zero downtime, Zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions
SV.TR.007	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs
SV.TR.008	Create a cluster out of multiple storage data stores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time
SV.TR.009	<ul style="list-style-type: none"> <li>VM-level encryption with no modifications in guest OS to protect unauthorized data access both at-rest and in-motion. The solution should also provide secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.</li> <li>Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions</li> </ul>
SV.TR.010	<ul style="list-style-type: none"> <li>Support boot from iSCSI, FCoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions</li> </ul>
SV.TR.011	<ul style="list-style-type: none"> <li>Span across a virtual datacentre and multiple hosts should be able to connect to it. This shall simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.</li> <li>In-built enhanced host-level packet capture tool which shall provide functionalities like SPAN, RSPAN, and ERSPAN and shall capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details</li> </ul>
SV.TR.012	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes
SV.TR.013	Simple and cost-effective backup and recovery for virtual machines which should allow admins to back up virtual machine data to disk without the need of agents and this backup solution should have built-in variable length de-duplication capability
SV.TR.014	<ul style="list-style-type: none"> <li>Solution should provide DR automation solution delivered from virtualization manager console for automated failover, fallback</li> </ul>

S. No.	Minimum Requirement Description
	<p>and recovery of application VMs in proper sequence to other data center with single click</p> <ul style="list-style-type: none"> <li>• Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment.</li> </ul>
SV.TR.015	<ul style="list-style-type: none"> <li>• Direct OEM 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates.</li> </ul>
SV.TR.016	<ul style="list-style-type: none"> <li>• It should include proactive smart alerts with self-learning performance analytics Capabilities with Prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behaviour, upcoming problems, and opportunities for efficiency improvements.</li> <li>• Capacity analytics which can identify over-provisioned resources so that they can be right-sized and "What If" scenarios to eliminate the need for spreadsheets, scripts and rules of thumb, as well as Real-time, integrated dashboards of performance and capacity to enable a proactive management approach and help ensure SLAs are met</li> <li>• Automated workflow triggers which would let admins associate workflows created in Orchestrator layer with Operations alerts. For example, these workflows can automatically delete old VM snapshots when available capacity falls below a critical threshold or add resources when workload demands are rising above normal</li> </ul>

#### 8.2.10 Network and Security Virtualization

S. No.	Minimum Requirement Description
NVS.TR.001	Solution should be integrated with proposed virtualization solution so that it should allow for automated and on-demand creation of Security policies which is scalable in nature.
NVS.TR.002	Solution should enable creation of security groups and security policies/rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc.
NVS.TR.003	The security policies should follow the Virtual Machines as they move within and between the virtual infrastructures so that there is no need of creation of security policies again for the applications once they move inside the datacentre.
NVS.TR.004	Solution should protect every Virtual Machine with a state full distributed firewall.
NVS.TR.005	Solution should provide efficient service chaining for providing advanced security with Virtual IPS, Firewall for Applications.
NVS.TR.006	The software defined security solution should provide integration with other security vendors who can host their virtual Firewall, IPS etc. onto the platform and should provide a centralized dashboard which can be used to automate the deployment of these 3rd party products across the underlying infrastructure. The solution should provide advanced service chaining and traffic steering capability.

S. No.	Minimum Requirement Description
NVS.TR.007	The solution should enable integration of third-party network and security solutions through open architecture and standard APIs. The bidder shall provide a list of ecosystem vendors that integrate with the framework
NVS.TR.008	The firewall-rule table of the solution should be designed for ease of use and automation with virtualized objects for simple and reliable policy creation
NVS.TR.009	The solution should provide embedded distributed firewall and should provide near line rate performance

### 8.2.11 Building Management System

S. No.	Minimum Requirement Description
BMS.TR.001	Solution for BMS: Solution should provide an appliance based pre-integrated, centralized and consolidated platform for end to end management of a building, which includes Facility infrastructure (HVACs, LT Panel- AMF, DG, UPS, Fuel Tank, CCTV, Fire Alarm and suppression system) along with IT infrastructure (network, server, application and database). The system should have the service dependency engine that allows to take intelligent decisions, as per the requirements. The tool should have the service oriented architecture layer and the mediation layer in a single plane. BMS should be open for third party integration via (soap, xml, web service, snmp-v1, v, v3), NO/NC ports (IO ports) and Modbus (TCP/IP&RTU) integration should be standard. For other industrial protocols, gateway integration should be available. The solution should perform the following general functions. But should be scalable with ready device certifications to accommodate new infrastructure getting added to the building
BMS.TR.003	Visibility - It should get a single platform to manage the entire building and its components along with the integration with IT infrastructure. The way ahead should be drilling down to the component, which is under performing / about to fail or has failed. The impact of the failed equipment on others should get highlighted. We should get a Hawkeye view to know, how are all the building components working at any point of time. So that issues are addressed as quickly as possible.
BMS.TR.004	Capacity Planning -End equipment's in the building, should be set with thresholds to get an idea of how well they are rendering services to the people in the building. It should be able to proactively identify potential areas which may need to be upgraded/downgraded (cooling, power, storage, etc.) with time. All vendor (end equipment vendors) SLA's and their respective maintenance contracts would be part of the OMS (operations and maintenance) plan.
BMS.TR.005	Third Party Integration - for seamless data sharing to build a "Collaborative Decision Making System".
BMS.TR.006	Salient Dependencies - Monitor & Control salient interdependencies between safety and security systems like: In case of fire, other than a fire alarm, we could get confirmatory information from the zonal camera. Multiple current surges in any particular zone should lead to an inspection of the electrical cables in the zone. Any sectional power failure, should help us to find the failure of the end equipment, by tracing down the LT panel SLD to the end equipment.

S. No.	Minimum Requirement Description
BMS.TR.007	System with CMDB - Integrate people, process & technology. Decreasing the likelihood of downtime in the building by facilitating communication across all equipment's (part of the facility). A definite inventory management tool with a workflow system connecting responsible people, should be part of the solution.
BMS.TR.008	Root-Cause Analysis - Isolate and pinpoint problem area before it impacts the building operations & business continuity while suppressing down the unwanted events.
BMS.TR.009	Energy sources should always keep in check on the rated power consumption vs the power available for consumption. Since one of the big reasons for fire is higher load than the power distribution capability.
BMS.TR.010	The solution should be capable to store the raw data or as-polled data, for minimum of 365 days. It should also have the facility to automate the backup process or allow us to take manual backup, in case required.
BMS.TR.011	The system should be capable of getting supported by the administrators at different levels. The system should provide individual and group rights and privileges. Normal users may have read access only, that too only to specific areas.
BMS.TR.012	Support for email and SMS both (integration with SMS-gateway and GSM communication).
<b>Energy Management</b>	
BMS.TR.014	The system should be capable of integrating with the mains (LT panel), DG, UPS, PDU, rectifier, energy meters for continuous monitoring of its health. The battery health of the UPS would also be needed.
BMS.TR.015	System should be able to do continuously monitor the quality of power, supplied to the electricity board and by the Generators (PF, frequency, harmonics distortion etc.), in order to avoid downtime.
BMS.TR.016	System should have the feature to setup thresholds on each of the monitored energy parameter.
BMS.TR.017	System should be able to clearly provide load trend for each rack, if need be in the building which would enable setup practical thresholds to get alerted on overload situations, in order to avoid any breakdown.
<b>Fire Alarm System Monitoring and Management</b>	
BMS.TR.018	The solution should proactively alert in case there is a possibility of an electrical fire (short circuit or over current)
BMS.TR.019	The solution should have the capability to integrate with different makes of fire alarm panels in the DCs and provide the alarms generated by the system on the centralized dashboard.
BMS.TR.020	The solution should be able to process a proper evacuation plan in-case of fire using the in-build rules engine.
BMS.TR.021	Trigger Audio and Visual alarm
BMS.TR.022	Co-relate with the nearest camera in the site with the FAS zone.
<b>DG Monitoring &amp; Fuel Automation</b>	
BMS.TR.023	Proposed system should be able to integrate with diesel generators for measuring fuel level and run hours of the DG. System should also allow

S. No.	Minimum Requirement Description
	monitoring of various alarms (like: LLOP, dg on, etc.) including quality of power of the DG.
BMS.TR.024	System should be capable to do fuel level monitoring of the diesel tanks installed for the gen-sets in the DC' building, in order to have a proactive estimation of fuel availability.
BMS.TR.025	
	Parameters - Generator and Fuel supply Automation Mains Fail DG On DG Failed to start DG Failed to stop DG Fuel Level Low High Water Temperature High Coolant Temperature Low Battery Voltage Low Lube Oil Pressure(LLOP)
Centralized Reporting & Dashboard	
BMS.TR.026	The dash board and reporting engine should provide centralized view for the entire infrastructure (physical security, safety & energy) and IT infrastructure (network, server, application and database) in the building.
BMS.TR.027	It should provide business users with highly interactive and power-users with highly sophisticated, pixel-perfect reports.
BMS.TR.028	It should provide Web-based interactive reporting for business users, Rich graphical report designer for power users, Parameterized reports with powerful charting, Output in popular formats: HTML, CSV, PDF, ASCII.
BMS.TR.029	It should provide Analysis to explore data by multiple dimensions such as customer, product, network and time into the hands of business users.
BMS.TR.030	It should provide intuitive & rich graphic designer to create customized reports.
BMS.TR.031	Solution should provide a comprehensive centralized dashboard for health monitoring of Infrastructure components like: Electrical Panels, HVAC, UPS, DG, Fuel etc. along with network, server, application and database.

### 8.2.12 Central Environment System

S. No.	Nature of requirement	Minimum Requirement Specifications
CES-FR-01	General	Environmental sensor station shall have a pre-installed software
CES-FR-02	General	Citizen can check the parameters through VaMS and Mobile App
CES-FR-03	General	System should give consolidated dashboard at City Operation Center of ASCL
CES-FR-04	Application	System should be able to integrate with existing Environment sensors and (if applicable), and showcase a consolidated dashboard to ASCL
CES-FR-05	Application	The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the

S. No.	Nature of requirement	Minimum Requirement Specifications
		data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.
CES-FR-06	Application	Software shall display real time and historical data in chart and table views for dashboard view of the Client.
CES-FR-07	Application	Software shall display trends of environmental parameters based on user specific time periods.
CES-FR-08	Application	It shall be possible to configure and calibrate the sensors through the software from a remote location.
CES-FR-09	Application	Alarms shall be generated for events where the environmental parameters breach the safe or normal levels.
CES-FR-10	Integration	The integrated DDS software application shall allow user to publish specific messages & general informative messages.
CES-FR-11	VAMS	VaMS shall be integrated with the environmental station for automatically displaying information from environmental sensors.
CES-FR-12	VAMS	VaMS software application shall provide the normal operator to publish predefined sets of messages (textual / image) along with information from environmental sensors. The application shall have an option for supervisor (someone with appropriate authority) to bypass the control during certain situations and to write in free-text mode.
CES-FR-13	Mobile App	System should be integrated with the Smart City App, where a Citizen can view the air quality, weather, sound, UV and other existing parameters

### 8.2.13 Video Management System

S. No.	Nature of requirement	Minimum Requirement Specifications
VMS-FR-01	General Requirements	VMS shall work on ONVIF Open Platform catering to all the security needs of the city
VMS-FR-02	General Requirements	VMS shall be open to any ONVIF IP cameras integration so that it would be able to cater future requirements of the project
VMS-FR-03	General Requirements	VMS shall support interoperability of IP cameras from multiple suppliers / vendors
VMS-FR-04	General Requirements	Bidders shall clearly mention in their proposal the brands and models integrated into VMS
VMS-FR-05	General Requirements	The VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.

S. No.	Nature of requirement	Minimum Requirement Specifications
VMS-FR-06	General Requirements	The VMS system shall cluster the processing & memory load across several machines. The failure of any one server in the solution shall not cause a failure in the entire system.
VMS-FR-07	General Requirements	The system shall allow the frame rate, bit rate and resolution of each camera to be configured independently for recording.
VMS-FR-08	General Requirements	The system shall support H.265 and MJPEG compression formats for all IP cameras connected to the system.
VMS-FR-09	General Requirements	The Video Management System shall support high availability of recording servers. A failover option shall provide standby support for recording servers with automatic synchronization to ensure maximum uptime and minimum risk of lost data.
VMS-FR-10	General Requirements	The Video Management System software shall have multicast and multi-streaming support. It shall definitely have the ability to take a snapshot from any online live camera and export to a standard graphic file format.
VMS-FR-11	General Requirements	The Video Management System shall support archiving for optimizing recorded data storage through unique data storage solutions by combining performance and scalability with cost efficient long-term video storage.
VMS-FR-12	General Requirements	The Video Management System shall incorporate intuitive map functions allowing for multi layered map environment. The map functionality shall allow for the interactive control of the complete surveillance system, at-a-glance overview of system integrity, and seamless drag-and-drop integration with video wall module option.
VMS-FR-13	General Requirements	The System should support Maps integration with below features:
VMS-FR-14		i. Adding Image Layers to the location map
VMS-FR-15		ii. Define the location map for each location
VMS-FR-16		iii. Add cameras to the map images
VMS-FR-17		iv. Add image layers to the map
VMS-FR-18		v. Add a Maps Server
VMS-FR-19		vi. System should support raster format images of jpeg/jpg and png file and Vector (shape files)
VMS-FR-20	General Requirements	The Video Management System shall incorporate fully integrated matrix functionality for distributed viewing of any camera in the system from any computer with the client viewer.
VMS-FR-21	General Requirements	VMS shall be ONVIF compatible

S. No.	Nature of requirement	Minimum Requirement Specifications
VMS-FR-22	General Requirements	VMS shall be scalable to support minimum 5000 or more cameras, which can be added into the system by only addition of software licenses and servers
VMS-FR-23	General Requirements	It shall be possible to integrate VMS into the Command & Control system. In that respect bidders shall provide their SDK/API (or any other integration means) libraries and documentation to ensure a seamless integration with any other system.
VMS-FR-24	General Requirements	VMS shall be open to any standard storage technologies integration.
VMS-FR-25	General Requirements	VMS shall already support Storage system from multiple vendors.
VMS-FR-26	General Requirements	VMS shall provide the ability to save any event that was tagged as an alarm (video motion detection, video loss or input) received, to be saved in a manner in which it cannot be overwritten.
VMS-FR-27	General Requirements	VMS shall be open to any video wall system integration
VMS-FR-28	General Requirements	VMS shall offer the possibility to integrate external Video Analytics systems.
VMS-FR-29	Distributed Architecture	It shall be possible to access VMS without installing dedicated client software (e.g. through the use of common web browser such as Internet Explorer...)
VMS-FR-30	Distributed Architecture	VMS shall be designed to offer a full IP based distributed architecture
VMS-FR-31	Distributed Architecture	VMS shall have the capability to handle software clients (operators) connected in different locations on the same network.
VMS-FR-32	Distributed Architecture	Simultaneous quantity of operators per location shall not be limited
VMS-FR-33	Management	VMS shall store the system's configuration in a relational database, either on the management server computer or on the network.
VMS-FR-34	Management	VMS shall authenticate user access, user rights and privileges of all operators through Active Directory
VMS-FR-35	Management	Access rights and privileges shall consist in but not limited to
VMS-FR-36		Visibility of devices, live view, playback, AVI/ ASF/ MP4 export, JPEG export, database export, sequences, smart search, input status, output control.
VMS-FR-37		PTZ control, PTZ priority, PTZ pre-set control
VMS-FR-38		Smart/Remote Client, live playback/setup, status API, service
VMS-FR-39		registration API and
VMS-FR-40		Privileges for the map feature
VMS-FR-41	Management	Registration of the system shall allow for on line activation and off line activation of licenses

S. No.	Nature of requirement	Minimum Requirement Specifications
VMS-FR-42	Management	The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by one Failover Server as a standby unit for max. 5 servers that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online
VMS-FR-43	Management	VMS shall operate in multicast / unicast / bandwidth throttling protocol to minimize the network bandwidth
VMS-FR-44	Multicasting	VMS shall support video streams up to at least 30 FPS
VMS-FR-45	Multicasting	Monitoring module shall allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices.
VMS-FR-46	Monitoring Module	The Monitoring module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
VMS-FR-47	Monitoring Module	Module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
VMS-FR-48	Monitoring Module	Viewing live video from cameras on the surveillance system with Playback recordings from cameras on the surveillance system, with a selection of advanced navigation tools, including an intuitive timeline browser.
VMS-FR-49	Monitoring Module	The system shall allow views to be created which are only accessible to the user, or to groups of users based on different layouts optimized for 4:3 and 16:9 display ratios. It should be able to create and switch between an unlimited number of views and able to display video from up to 64 cameras from multiple servers at a time.
VMS-FR-50	VMS Storage	It shall be possible to schedule recording and archiving by a recurrence pattern (daily, weekly, specific time and dates) and by specific time ranges (all day, time range, daytime, night time...)
VMS-FR-51	VMS Storage	It shall be possible to schedule recording on per camera basis (Continuous, manual or motion based)
VMS-FR-52	VMS Storage	It shall be possible to schedule recording on per camera basis (Continuous, manual or motion based)
VMS-FR-53	VMS Storage	VMS shall allow the control of the amount of used disk space.
VMS-FR-54	VMS Storage	It shall be possible to protect specific video streams against any deletion and for any period of time

S. No.	Nature of requirement	Minimum Requirement Specifications
VMS-FR-55	Log Management	The system log shall be searchable by Level, Source and Event Type.
VMS-FR-56	Log Management	The Alert Log records alerts triggered by rules (searchable by Alert type, Source and Event type)
VMS-FR-57	Management	The system shall have smart recording wherein no recording or recording at lower frame rate is done when there is no movement. The VMS shall be able to record higher-quality video and shall reduce fps when not in use during Night time.
VMS-FR-58	Management	System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.
VMS-FR-59	Management	System should support thumbnail search to quickly locate specific scenes or events in recorded video without fast-forwarding or rewinding. Thumbnail Search should display a range of video as thumbnail images, should allow to identify a portion of the recording to review.
VMS-FR-60	Management	System should support Clip Management—Use Clip Management to view, download and delete clips. That are stored on the server.
VMS-FR-61	Management	No. of operators shall not be software licenses dependent. In case of emergency situation, threats, natural catastrophe the control room shall be able to reconfigure the VMS by adding more operators without any Contractor's intervention.
VMS-FR-62	Management	Security Platform shall have strong security mechanism such as the use of advance encryption, digital certificates and claims-based authentication to ensure that only authorised personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.

#### 8.2.14 Video Analytics

S. No.	Nature of requirement	Minimum Requirement Specifications
VCA-FR-01	General Requirements	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
VCA-FR-02	General Requirements	The system shall provide configurable detection zones and lines to detect events of interest, Detection zones define an area of interest and Detection lines define a perimeter instead of a region.
VCA-FR-03	General Requirements	The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts

S. No.	Nature of requirement	Minimum Requirement Specifications
VCA-FR-04	General Requirements	The system shall allow the configuration of applicable rules and manage them.
VCA-FR-05	General Requirements	The system shall also enable editing the Zones and lines to the desired shape or size.
VCA-FR-06	General Requirements	The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a yellow coloured target changing the colour to red on event
VCA-FR-07	General Requirements	The system shall enable masking of areas which interfere detection zones in other areas of the scene
VCA-FR-08	General Requirements	The system shall enable detecting rules in the defined areas (zones/ lines)
VCA-FR-09	General Requirements	The system shall provide a functionality for configuring timelines for various events such as abandoned object, camera tampering etc.
VCA-FR-10	General Requirements	The system shall be able to filter large amounts of video and focus on human attention appropriately
VCA-FR-11	General Requirements	The system shall allow classification of different objects like animals, vehicles, people etc.
VCA-FR-12	General Requirements	The System shall have Automated PTZ camera control for zooming in on interesting events like motion Detection etc. as picked up by Camera without the need for human intervention.
VCA-FR-13	General Requirements	VCA shall provide secured feeds with encryption, watermarking for data authenticity
VCA-FR-14	General Requirements	VCA shall be able to trigger alerts for the vehicle direction, vehicle speed, vehicle parked in defined zones etc.
VCA-FR-15	General Requirements	The system shall have a reporting generation functionality to provide inputs on various instances of events triggered in the system
VCA-FR-16	General Requirements	VAS should allow to add, edit, delete or disable and enable Policies.
VCA-FR-17	Features	The city wide surveillance system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers. The solution should offer following triggers from Day1.
VCA-FR-18	Security Features	Camera Tampering (In case this is an inherent feature of the camera, this may not be provided as a separate line item in VA), Unattended object, Object Classification, Tripwire / Intrusion, Loitering, etc.
VCA-FR-19	Traffic / Parking Features	Vehicle Wrong Way Detection, Illegal Parking Detection, Congestion Detection, Vehicle Counting, Speeding Detection, Parking Management etc.

S. No.	Nature of requirement	Minimum Requirement Specifications
VCA-FR-20	Enhanced Monitoring Features	Video Stitching with Object Tracking, Video Stabilization, Video Smoke Detection, Video Fire Detection etc.
VCA-FR-21	Crowd Management	Crowd Control, Counter-Flow Detection, People Counting, Line Control, People Tracking etc.
VCA-FR-22	General Requirements	Motion Detection component that automatically detects moving objects in the field of view of a camera, and is capable of filtering out movement in configurable directions and movement due to camera motion (e.g. from wind)
VCA-FR-23	General Requirements	System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification
VCA-FR-24	Log Management	System should have a proper MIS system for recording of various video analytics as per need. There should be provisions for acknowledging the events with remarks in the system itself & print out of a period specific list can be taken for recording purpose.

#### 8.2.15 Face Recognition System Software

S. No.	Nature of requirement	Minimum Requirement Specifications
FRS-FR-01	General Requirements	The facial recognition system should be able to integrate with IP Video Cameras as required in the solution and shall be able to identify multiple persons of interest in real-time, through leading-edge face recognition technology. The system shall be able to recognize subjects appearing simultaneously in multiple live video streams retrieved from IP surveillance cameras. The Facial recognition system should seamlessly be integrated to the network video recorders and the video management system.
FRS-FR-02	General Requirements	The facial recognition system should be able to work on the server/ desktop OS as recommended by OEM and provided by the Master System Integrator
FRS-FR-03	General Requirements	The user interface of the facial recognition system should have a report management tool without installation of any additional client software. It should be able to generate real time report such as Audit log report, Hit List Report, Daily Statistics Report and Distribution Report etc.
FRS-FR-04	General Requirements	The facial recognition system should be accessible from 5 different desktops / laptops at any given time. When choosing a distributed architecture, the system

S. No.	Nature of requirement	Minimum Requirement Specifications
		shall be able to completely centralize the events and galleries from each local station into a unique central station, devoted to management and supervision.
FRS-FR-05	General Requirements	The system should have ability to handle initial real-time watch list of 10,000 Faces (should be scalable to at least 1 Million faces) and 50 Camera Feeds simultaneously and generate face matching alerts.
FRS-FR-06	General Requirements	The algorithm for facial recognition or the forensic tool should be able to recognise partial faces with varying angles
FRS-FR-07	General Requirements	The system should be able to detect multiple faces from live single video feed
FRS-FR-08	General Requirements	The system should have combination of eye-zone extraction and facial recognition
FRS-FR-09	General Requirements	The system should have short processing time and high recognition rate
FRS-FR-10	General Requirements	The system should be able to recognize faces regardless of vantage point and any facial accessories/ hair (glasses, beard, expressions)
FRS-FR-11	General Requirements	Face detection algorithms, modes and search depths should be suitable for different environments such as fast detection, high accuracy etc.
FRS-FR-12		The FRS system shall use of GPU technology instead of Traditional CPUs, to greatly improve the computational performance in crowded environments.
FRS-FR-13	General Requirements	The system should be able to identify and authenticate based on individual facial features
FRS-FR-14	General Requirements	The system should be compatible with the video management system being proposed by the Master System Integrator
FRS-FR-15	General Requirements	The system should have capability for 1:1 verification and 1:N identification matching
FRS-FR-16	General Requirements	The system should be able to integrate with other systems in the future such as 'Automatic fingerprint identification system (AFIS)' etc.
FRS-FR-17	General Requirements	The system should be able to support diverse industry standard graphic and video formats as well as live cameras
FRS-FR-18	General Requirements	The system should be able to match faces from recorded media.
FRS-FR-19	General Requirements	The system should be able to detect a face from a group photo

S. No.	Nature of requirement	Minimum Requirement Specifications
FRS-FR-20	General Requirements	The system should be able to detect a face from stored videos of any format
FRS-FR-21	General Requirements	The system should have bulk process of adding faces in the system
FRS-FR-22	General Requirements	The system should be an independent system, with capability to integrate with industry standard Video Management Systems (VMS) for alert viewing.
FRS-FR-23	General Requirements	The system should allow users to search or browse captured faces (based on date or time range), export any captured image for external use with a capability to support a Handheld mobile with app for windows OS or android OS to capture a face on the field and get the matching result from the backend server.
FRS-FR-24	General Requirements	The proposed solution should provide the ability to assign different security levels to people and places. It should alert security staff when someone is spotted in an area where they're not permitted, whilst allowing them free access to non-restricted/public areas.
FRS-FR-25	General Requirements	The system shall be able to detect faces in different environmental changes like rain, wind, fog and poor light.
FRS-FR-26	General Requirements	The system should have the facility to categorize the images like "Remember this person" or "hit-list" or "wanted".
FRS-FR-27	General Requirements	The OEM should have deployed the solution in India
FRS-FR-28	Features	FRS should cover the following features: i. Face Capture ii. Face Counting iii. Face Recognition
FRS-FR-29	General Requirements	Facial Image Database Management: It should allow users to manage the facial image library, including registering, changing, deleting & querying facial image information

### 8.2.16 ANPR Software

S. No.	Nature of Requirement	Minimum Requirement Specifications
ANPR-FR-01	Vehicle Detection and Video Capture Module	<ul style="list-style-type: none"> <li>- The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition.</li> </ul>

S. No.	Nature of Requirement	Minimum Requirement Specifications
		<ul style="list-style-type: none"> <li>• The System should automatically detect the license plate in the captured video feed in real-time.</li> <li>• The system should perform Optical Character Recognition (OCR) of the license plate characters.</li> <li>• The System should store JPEG image of vehicle and license plate and enter the license plate number into database management system like MSSQL, MySQL, PostgreSQL etc. along with date timestamp and site location details.</li> <li>• System should be able to detect and recognize the English alpha numeric license plate in standard fonts and formats for classes of vehicles such as cars, HCV, and LCV.</li> <li>• The system should be robust to variation in License Plates in terms of font, size, contrast and colour and should work with good accuracy</li> </ul>
ANPR-FR-02	Vehicle Detection by Colour	<ul style="list-style-type: none"> <li>• The system should detect the colour of all vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colours. The system should store the colour information of each vehicle along with the license plate information for each transaction in the database.</li> <li>• The system should have options to search historical records for post event analysis by the vehicle colour or the vehicle colour with license plate and date time combinations.</li> </ul>
ANPR-FR-03	Alert Generation	<ul style="list-style-type: none"> <li>• The system should have option to input certain license plates according to the hot listed categories like "Wanted", "Suspicious", "Stolen", etc. by authorized personnel.</li> <li>• The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories</li> </ul>
ANPR-FR-04	Vehicle Status Alarm Module	<ul style="list-style-type: none"> <li>• On successful recognition of the number plate, system should be able generate automatic alarm to alert the control room for vehicles</li> </ul>

S. No.	Nature of Requirement	Minimum Requirement Specifications
		<p>which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need).</p> <ul style="list-style-type: none"> <li>- The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user.</li> </ul>
ANPR-FR-05	Vehicle Log Module	<ul style="list-style-type: none"> <li>- The system should enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations.</li> <li>- The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports should include:</li> <li>- Report of vehicle flow at each of the installed locations for Last Day, Last Week and Last Month.</li> <li>- Report of vehicles in the detected categories at each of the installed locations for Last Day, Last Week and Last Month.</li> <li>- Report of Vehicle Status change in different Vehicle Categories.</li> <li>- The system should have Search option to tune the reports based on license plate number, date and time, site location as per the need of the authorities.</li> <li>- The system should have option to save custom reports for subsequent use. The system should have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems.</li> <li>- The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1 and 2-character distance).</li> </ul>
ANPR-FR-06	Vehicle Category Editor	<ul style="list-style-type: none"> <li>- The system should have option to input certain license plates according to category like "Wanted", "Suspicious", "Stolen", and "Expired" etc. by Authorized personnel.</li> </ul>

S. No.	Nature of Requirement	Minimum Requirement Specifications
		<ul style="list-style-type: none"> <li>• The system should have an option to add new category by authorized personnel.</li> <li>• The system should have option to update vehicle status in specific category by authorized personnel. E.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved".</li> <li>• System should have option to specify maximum time to retain vehicle records in specific categories.</li> </ul>
ANPR-FR-07	Central Management Module	<ul style="list-style-type: none"> <li>• The Central Management Module should run on the ANPRS Central Server in control booth. It should be possible to view records and edit hotlists from the Central Server</li> </ul>
ANPR-FR-08	Centralized Video Management Module	<ul style="list-style-type: none"> <li>• Besides recording the snaps &amp; video clips of every license plate extracted, it is also required that a centralized video management software is also supplied to achieve the below: -</li> <li>• Continuous recording of every lane video irrespective of presence of vehicle.</li> <li>• Such recording schedules can be continuous, event based, schedule based, trigger based etc.</li> <li>• Archive Search using dates, time, event etc.</li> <li>• High Availability/Redundancy of Recording &amp; Database.</li> <li>• Health monitoring module - To allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices. The health monitoring module should provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.</li> <li>• Virtual Matrix - To allow viewing of live video in different layouts on operator screen.</li> <li>• Video stitching - It should allow stitching of multiple lane videos/tiles to provide panoramic type seamless view of both entry &amp; exit lanes.</li> <li>• The centralized Video Management Module should be part of same ANPR software framework. No 3rd party VMS is allowed to be offered, howsoever integrated it may be</li> </ul>

### 8.2.17 Body Camera Software License

S. No.	Nature of Requirement	Minimum Requirement Specifications
BCS-TR-01	General	Body camera software can be provided as a Cloud-based platform, as a hybrid installation onto your existing server infrastructure or as a single, standalone install to a local PC or laptop. Software allows our solutions to be suitable for the largest, complex deployments of Body Worn Video or for single user applications
BCS-TR-02	Encryption	Software provides AES encryption, ensuring your files are completely secure, and a full audit trail to protect the evidential integrity of the videos you capture. Access to the software is password protected, and multiple user access levels can be allocated dependent on requirements
BCS-TR-03	Functionality	Searching and organising your files is completely intuitive. Files are sorted and searchable by vital metadata such as date, time, location, device number and user. You can also add your own tags to files to make them even easier to find
BCS-TR-04	Cloud-based	Access to the software is provided to your organisation via the internet. It requires no physical installation and all your files are stored securely in cloud. This solution is ideal if you need to access EMS from multiple locations and / or lack onsite supporting storage infrastructure
BCS-TR-05	Hybrid Install	Software will perform a custom install of EMS onto your organisation's server. This is ideal if you need to access EMS from multiple locations and have a preference to host the software on your own private network / robust onsite storage infrastructure
BCS-TR-06	Standalone	A single instance install of WCCTV's EMS onto your standalone PC or Laptop
BCS-TR-07	Scalable Platform	Cloud-based, Hybrid or Standalone Install
BCS-TR-08	Password protected	responsive and intuitive design, transfer and store your AES encrypted data
BCS-TR-09	Role based	Set designated administration levels and user access rights
BCS-TR-10	Manage your files	Organise and search for your files using detailed metadata
BCS-TR-11	Share	Collaborate on cases by securely sharing case files

S. No.	Nature of Requirement	Minimum Requirement Specifications
BCS-TR-12	Data Protection	Files are deleted after 30 days (configurable) unless required for ongoing case
BCS-TR-13	Evidential usage	Provides full audit trail so your files are evidentially sound

#### 8.2.18 Public Announcement Software License

S. No.	Category	Minimum Requirement Specifications
PAS-FR-01	General	<ul style="list-style-type: none"> <li>• Software shall be fully proven prior to being supplied, installed, tested and commissioned.</li> <li>• A list of reference sites at which the system software has been installed and operational at the date of the closing of this tender shall be provided.</li> <li>• The operator interface software shall incorporate English language descriptions and messages using both text based menus and graphical/icon displays. All configuration (e.g. entering of alarm response properties, adjusting time schedules, user data, etc.) shall be performed on-line without effecting the operation of the overall system.</li> <li>• Selective access to different operator functions shall be configured based on an operator's user level. User levels shall be determined from the Biometric verification each time an operator logs on to a workstation.</li> <li>• After any predefined period, if no operator activity has occurred at the operator workstations, that station shall automatically request Biometric verification failing which the station shall log off.</li> <li>• The time period before automatic logging off of workstations shall be user configurable, and shall be determined during commissioning of the system, in liaison with the Engineer.</li> </ul>
PAS-FR-02	Operating System	<ul style="list-style-type: none"> <li>• The operating system shall be a recognised and widely accepted standard operating</li> </ul>

S. No.	Category	Minimum Requirement Specifications
		<p>system that shall suit the requirements of the system to be installed. The operating system shall be a real time multi-user/multi-tasking system such as NT, W2000, Unix or QNX. The operating system shall have proven and demonstrated reliable operation in the security environment.</p> <ul style="list-style-type: none"> <li>Facilities shall be provided to store all programs on site and include all equipment necessary to backup and reload all system programs, including the operating system with all user specific system parameters.</li> </ul>
PAS-FR-03	System Access	<ul style="list-style-type: none"> <li>Operators shall be required to "log on" to operator workstations using the finger print reader provided at each operator station before being able to access the system or user information, reset alarms or access any other system functions.</li> <li>Access to all workstations shall be limited through allocation of access levels.</li> <li>A minimum of 100 users and 100 User levels shall be available. Only users allocated with a user level of 99 shall be capable of the assignment and changing of passwords to all levels.</li> <li>Each operator shall be allowed to access different operator commands and functions, and view certain individually assigned events, menus and functions based on their assigned user level.</li> </ul>
PAS-FR-04	System Reporting	<ul style="list-style-type: none"> <li>The GUI shall be capable of performing SQL queries to the current or archived databases on the server workstations, format the data into customised reports which shall allow for the following:</li> <li>Display of all relevant information on any individual alarm point including alarm point identification by device number and alarm point status.</li> <li>Display all alarm points in the system in alarm or normal condition, as a single log.</li> <li>Display all emergency procedures applicable to any alarm type with corresponding alarm</li> </ul>

S. No.	Category	Minimum Requirement Specifications
		<p>response actions and locations, per alarm device.</p> <ul style="list-style-type: none"> <li>• Reporting details shall include:</li> <li>• Alarm point status</li> <li>• Alarm count per device.</li> <li>• Alarm activity over a time period, selected by time and date.</li> <li>• Display of selected alarm transactions based on alarm type and a calendar / time period.</li> <li>• Display system operators login/out history</li> <li>• Display all operator commands entered by any or all operators based on time/calendar interval.</li> </ul>
PAS-FR-04	System Status	<ul style="list-style-type: none"> <li>• The GUI shall provide a menu option which, when selected, allows the system to display or print a list of current alarms, faults and conditions including the current fault conditions relating to GUI workstations and Intercom system hardware.</li> <li>• In graphical display mode the system shall display maps of each building complete with all internal levels and shall indicate all systems equipment status (i.e. Intercom on, off, tamper, Threshold, isolated etc.)</li> </ul>

#### 8.2.19 Fleet Tracking Software

S. No.	Indicative Requirement Description
FMS.TR.001	The fleet tracking solution shall allow Real time location tracking of all vehicles including those for Police, Fire, SWM Bin Collection, D2D Collection operations etc. on the city on map.
FMS.TR.002	The system shall provide Real-time status of engine of the vehicle i.e. running, stopped
FMS.TR.003	The system shall provide Real-Time status of battery supply from vehicle
FMS.TR.004	The system shall provide Vehicle Navigation for fixed routes to be completed by vehicles with audio in Punjabi, Hindi and English mounted on vehicle dashboard.
FMS.TR.005	The system shall provide ability to assign fixed routes on daily basis to all registered vehicles in system with bin collection or feeder points along the route and track any deviation from fixed routes allocated.
FMS.TR.006	The system shall provide ability trace vehicle breakdown events, driver unavailability to maintain service levels in the city based on vehicle missing pick-up schedules.

S. No.	Indicative Requirement Description
FMS.TR.007	The system shall provide ability to re-assign drivers to vehicles and routes based on their availability
FMS.TR.008	The system shall provide to do geo-fencing of vehicles to restrict area of operation in specified hours during the day.
FMS.TR.009	The system shall provide ability to monitor entry and exit time of vehicles in garages, depots, transfer stations, landfills etc. in the city
FMS.TR.010	The system shall provide ability to keep track of schedule for servicing of all bin locations in the city for waste collection
FMS.TR.011	The system shall provide ability to keeping track of schedule for servicing of all D2D Collection Feeder points in the city for waste collection

### 8.2.20 OWQMS Web Application

S. No.	Nature of requirement	Minimum Requirement Specifications
On-line waste water Quality Monitoring System (OWQMS)		
OWQMS-FR-01.1	General	OWQMS shall consist of a web based application and mobile application to provide systematic framework for enhancing waste water discharge monitoring to detect emerging water quality issues and respond prior to the problem occurs in the city.
OWQMS-FR-01.2		OWQMS shall utilize real-time water quality parameters collected from quality sensors across the drainage canals to analyse and detect waste water quality anomalies.
OWQMS-FR-01.3		Monitoring shall include all the waste water quality parameters received from the remote sensors.
OWQMS-FR-01.4	Data Communication	Waste water quality parameters shall be fetched from the Intelligent Gateway via 3G/LTE network.
OWQMS-FR-01.5		The system shall have the desired interfaces for the data integration with other existing applications as necessary. It shall be possible to integrate with State and Central pollution Boards portals/database via API integration to share waste water quality data.
OWQMS-FR-01.6		The application shall import and store sensor measurement and state data (operational and communication status) at a specified time frequency from other relevant databases and systems to analyse, and visualize the waste water quality data on a continuous basis.
OWQMS -FR-01.7	Information Management & Analysis	Based on operational and communication status and other characteristics, it shall determine whether data is valid or invalid,

S. No.	Nature of requirement	Minimum Requirement Specifications
		and whether the quality of the data is sufficient to assess waste water quality.
OWQMS-FR-01.8		Shall analyse valid sensor data to assess water quality and sensor states.
OWQMS-FR-01.9		Shall perform advanced data analysis, such as time-series trend analysis, multi-parameter clustering, and single parameter thresholding for identifying unusual waste water quality events due to either intentional or unintentional causes
OWQMS -FR-01.10	Alert Investigation	Shall generate and manage alarms based on sensor states and waste water quality determined by the analysis of a) valid sensor data and b) calculated water quality parameters
OWQMS -FR-01.11		Shall generate email and sms notifications, follow-up notifications, and escalated notifications to appropriate personnel in the event of alarms
OWQMS -FR-01.12		Shall generate standard and user-configured reports.
OWQMS -FR-01.13	Reports	Shall have the control access to all data, results, reports, and system administration tools

#### 8.2.21 Anti-Virus Solution

S. No.	Minimum Requirement Description
AVS.TR.001	Anti-virus shall have auto update feature, it shall be able to push signature from the centralized server to all the clients Or workstations
AVS.TR.002	Bidder shall ensure that the scan logs are made available for review.
AVS.TR.003	The solution must support mass mailing virus detection.
AVS.TR.004	The solution must support mail attachment virus detection.
AVS.TR.005	The solution must support Malformed Mail format detection.
AVS.TR.006	The solution must have a built in Safe Stamp feature to have a sign of a secure email. The email scanning time stamp shows whether the sender's antivirus database is not up to date or not.
AVS.TR.007	The solution must have its own Updated Recommended Virus Extensions.
AVS.TR.008	The solution must support Heuristics-based mail header detection for Spam.
AVS.TR.009	The solution must support Heuristics-based scanning of the mail body for Spam.
AVS.TR.010	The solution must support administrator defined Anti-Spam exception list (approved list).
AVS.TR.011	The solution must support administrator to define list of known spammers.
AVS.TR.012	The solution shall be able to detect Spam in form of categories like general, commercial email, Get rich quick, pornography etc.

S. No.	Minimum Requirement Description
AVS.TR.013	The solution shall be able to take action based on the category in which Spam is detected.
AVS.TR.014	The solution must be able to take different action based on the different sensitivity level of Spam detection.
AVS.TR.015	The solution must provide alerts based on action taken on the Spam mail.
AVS.TR.016	The solution must support Encrypted Mail Detection.
AVS.TR.017	The solution must support Password Protect Zip Detection.
AVS.TR.018	The solution must have a Secure SSL Web Management Console.
AVS.TR.019	The solution must be able to prevent System Denial of Service ('Do's') Attack.
AVS.TR.020	Bidder shall propose the required hardware for the entire solution
AVS.TR.021	Bidder shall provide requisite licenses for all the software required for the Anti-virus and Anti-spam Solution.
AVS.TR.022	Solution should provide protection against Back Doors and Trojan Horses
AVS.TR.023	Solution should provide real time fraud and risk management including but not limited to behavioural analysis, key loggers, Trojans and should allow monitoring on transactions and raise alerts in case of suspicious activities as defined by the security policy of organization.

#### 8.2.22 Web based Helpdesk & Incident Management Software with Application / Platform / OS Licenses

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-01	General Attributes	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 software 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.
WBH-FR-02	General Attributes	Bidder is required to design, supply, install, customize, test, implement, rollout and maintain the helpdesk application and hardware as per the requirements of this RFP. The proposed helpdesk solution shall provide comprehensive and end-to-end management of all the components for each service including all the hardware devices, Network, Systems and Application infrastructure.
WBH-FR-03	General Attributes	Bidder is expected to provide helpdesk encompassing but not limited to the following functions: <ul style="list-style-type: none"> <li>• Configuration Management</li> <li>• Fault Management</li> <li>• Incident, Problem and Change Management</li> <li>• Asset Management</li> </ul>

S. No.	Nature of Requirement	Minimum Requirement Specifications
		<ul style="list-style-type: none"> <li>• Remote Control</li> <li>• SLA Management &amp; Monitoring</li> <li>• Performance Management</li> <li>• Monitoring Backup and Management</li> <li>• Event Management</li> <li>• Server, Storage and other Infrastructure Management</li> <li>• Monitor network components of the LAN &amp; WAN</li> <li>• Network Link Monitoring</li> </ul> <p>Any other modules as required by SI to meet the requirements of the RFP All EMS modules required to fulfil the requirements laid in the RFP should necessarily be from single OEM only.</p> <p>Note: It is mandatory that all the modules for the proposed EMS Solution shall provide out-of-the-box and seamless integration capabilities. Bidder shall provide the specifications and numbers for all necessary Hardware, OS &amp; DB (if any) which is required for an EMS to operate effectively and provide the same at no extra cost.</p>
WBH-FR-04	General Attributes	<p>Following functionalities are essential and required from such EMS tools:</p> <ul style="list-style-type: none"> <li>• Availability Monitoring, Management and Reporting</li> <li>• Performance Monitoring, Management and Reporting</li> <li>• Helpdesk Monitoring, Management and Reporting</li> <li>• Asset Management</li> <li>• Incident Management and RCA reporting</li> <li>• Change and Configuration management</li> </ul>
WBH-FR-05	Discovery, Configuration and Faults: Monitoring and Management	The proposed system shall support multiple types of discovery like IP range discovery including built-in support for IPv6 , Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices
WBH-FR-06	Discovery, Configuration and Faults: Monitoring and Management	The proposed system shall support exclusion of specific IP addresses or IP address ranges.
WBH-FR-07	Discovery, Configuration and Faults: Monitoring and Management	The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-08	Discovery, Configuration and Faults: Monitoring and Management	The discovery shall be able to identify and model of the ICT asset.
WBH-FR-09	Discovery, Configuration and Faults: Monitoring and Management	The proposed system shall provide a detailed asset report, organized by system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.
WBH-FR-10	Monitoring and Management	The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason.
WBH-FR-11	Monitoring and Management	The proposed system shall provide out of the box root cause analysis.
WBH-FR-12	Monitoring and Management	The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
WBH-FR-13	Monitoring and Management	The proposed solution shall detect virtual server and virtual machine configuration changes and automatically update topology and shall raise alarm when VM migrations happen between hosts.
WBH-FR-14	Monitoring and Management	The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.
WBH-FR-15	Monitoring and Management	The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.
WBH-FR-16	Monitoring and Management	The proposed system shall support SNMPv3-based network discovery and management out-of-box without the need for any external third-party modules.
WBH-FR-17	Monitoring and Management	The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & start-up configuration, Upload configuration etc.
WBH-FR-18	Reporting	The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-19	Reporting	The proposed system shall able to perform real-time or scheduled capture of device configurations. It shall also provide features to capture, view & upload network device configuration.
WBH-FR-20	Reporting	The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.
WBH-FR-21	Reporting	The proposed system shall be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
WBH-FR-22	Reporting	The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.
WBH-FR-23	Service Level Management: Monitoring and Management	The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the component and services provisioned as well as the SLAs.
WBH-FR-24	Service Level Management	The system shall provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
WBH-FR-25	Service Level Management	The system shall be capable of managing IT and Non-IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.
WBH-FR-26	Service Level Management	The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).
WBH-FR-27	Service Level Management	SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.
WBH-FR-28	Service Level Management	The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In

S. No.	Nature of Requirement	Minimum Requirement Specifications
		addition the capability to exempt any service outage from impacting an SLA shall be available.
WBH-FR-29	Service Level Management: Reporting	The reports supported shall include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
WBH-FR-30	Service Level Management: Reporting	The system shall provide a historical reporting facility that shall allow for the generation of on-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.
WBH-FR-31	Service Level Management: Reporting	The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box.
WBH-FR-32	Service Level Management: Reporting	The System shall have all the capabilities of a Network Management System which shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.
WBH-FR-33	Network Performance Monitoring, Management and Reporting: Monitoring and Management	The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.
WBH-FR-34	Network Performance Monitoring, Management and Reporting: Monitoring and Management	The tool shall have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices
WBH-FR-35	Network Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall use intelligent alarm algorithms to learn the behaviour of the network infrastructure components over a period of time
WBH-FR-36	Network Performance Monitoring, Management and Reporting:	The Network Performance Management console shall provide a consistent report generation interface from a single central console.

S. No.	Nature of Requirement	Minimum Requirement Specifications
	Reporting	
WBH-FR-37	Network Performance Monitoring, Management and Reporting: Reporting	This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.
WBH-FR-38	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall enable complete customization flexibility of performance reports for network devices and monitored servers.
WBH-FR-39	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.
WBH-FR-40	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems quickly. The following charts like mentioned below shall be available for routers: Backplane Utilization, Buffer Create Failures, Buffer Hits, Buffer Misses, Buffer Utilization, Bus Drops, CPU Utilization, Fan Status, Free Memory, Memory Utilization, Packets by Protocol, and Packets out.
WBH-FR-41	Network Performance Monitoring, Management and Reporting: Reporting	The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.
WBH-FR-42	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall proactively monitor all user transactions for any web-application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes
WBH-FR-43	Application Performance Monitoring, Management and Reporting:	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.

S. No.	Nature of Requirement	Minimum Requirement Specifications
	Monitoring and Management	
WBH-FR-44	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall correlate performance data from HTTP Servers (external requests) with internal application performance data.
WBH-FR-45	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall see response times based on different call parameters. For example the proposed solution shall be able to provide CPU utilization metrics.
WBH-FR-46	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed Solution shall be able to correlate Application changes (code and configuration files) with change in Application performance.
WBH-FR-47	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall allow data to be seen only by those with a need to know and limit access by user roles.
WBH-FR-48	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall measure the end users' experiences based on transactions.
WBH-FR-49	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall give visibility into user experience without the need to install agents on user desktops.
WBH-FR-50	Application Performance Monitoring, Management and	The solution shall be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.

S. No.	Nature of Requirement	Minimum Requirement Specifications
	Reporting: Monitoring and Management	
WBH-FR-51	Application Performance Monitoring, Management and Reporting: Monitoring and Management	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.
WBH-FR-52	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction
WBH-FR-53	Application Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the Data center without having to rely on network monitoring tools.
WBH-FR-54	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.
WBH-FR-55	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed system shall addresses management challenges by providing centralized management across physical and virtual systems. The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
WBH-FR-56	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-57	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
WBH-FR-58	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.
WBH-FR-59	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started.
WBH-FR-60	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to take action like sending an email.
WBH-FR-61	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.
WBH-FR-62	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	It shall be able to automate monitoring, data collection and analysis of performance from single point.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-63	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management	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.
WBH-FR-64	Systems and Database Performance Monitoring, Management and Reporting: Reporting	The proposed system shall provide Performance Management and Reporting Provides real-time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines.
WBH-FR-65	Systems and Database Performance Monitoring, Management and Reporting: Reporting	Role based Access Enables role-based management by defining access privileges according to the role of the user.
WBH-FR-66	Systems and Database Performance Monitoring, Management and Reporting: Reporting	The proposed Virtual Performance Management system shall integrate latest virtualization technologies
WBH-FR-67	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.
WBH-FR-68	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.
WBH-FR-69	Helpdesk - Monitoring, Management and Reporting	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-70	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.
WBH-FR-71	Helpdesk - Monitoring, Management and Reporting	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.
WBH-FR-72	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users. The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.
WBH-FR-73	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email, web etc.
WBH-FR-74	Helpdesk - Monitoring, Management and Reporting	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.
WBH-FR-75	Helpdesk - Monitoring, Management and Reporting	It shall support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
WBH-FR-76	Helpdesk - Monitoring, Management and Reporting	Remote desktop sharing in the system shall be agent less & all activity shall be automatically logged into the service desk ticket. It shall allow IT team to create solution & make them available on the end user login window for the most common requests
WBH-FR-77	Incident Management and Root Cause Analysis Reporting	Incident management shall be governed by the change management and configuration management policy of PCSCL. The policy shall be shared with the Bidder.
WBH-FR-78	Incident Management and Root Cause Analysis Reporting	An information security incident is an event (or chain of events) that compromises the confidentiality, integrity or availability of information. All information security incidents that

S. No.	Nature of Requirement	Minimum Requirement Specifications
		affect the information or systems of the enterprise (including malicious attacks, abuse / misuse of systems by staff, loss of power / communications services and errors by users or computer staff) shall be dealt with in accordance with a documented information security incident management process.
WBH-FR-79	Incident Management and Root Cause Analysis Reporting	Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.
WBH-FR-80	Incident Management and Root Cause Analysis Reporting	It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.
WBH-FR-81	Incident Management and Root Cause Analysis Reporting	Testing shall be performed to ensure that recovery action is complete and that the service has been fully restored. The Bidder shall keep the end users informed of the progress of their reported incident. 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.
WBH-FR-82	Incident Management and Root Cause Analysis Reporting	Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.
WBH-FR-83	Incident Management and Root Cause Analysis Reporting	The Bidder shall conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).
WBH-FR-84	Incident Management and Root Cause Analysis Reporting	The incident management activities shall be carried out by the Bidder in such a way that an incident is resolved within the agreed time schedule. Root Cause Analysis (RCA) shall be conducted by the Bidder.
WBH-FR-85	Incident Management and Root Cause Analysis Reporting	Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
WBH-FR-86	Change and Configuration Management	Change and configuration management shall be governed by the change management and configuration management policy.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-87	Change and Configuration Management	Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.
WBH-FR-88	Change and Configuration Management	All changes shall be initiated using change management process; and a Request For Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.
WBH-FR-89	Change and Configuration Management	The Bidder shall ensure that all changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled to track and report all changes.
WBH-FR-90	Change and Configuration Management	Ensure review of changes for effectiveness and take actions agreed with interested parties. Requests for change shall be analysed at planned intervals to detect trends. The results and conclusions drawn from the analysis shall be recorded and reviewed to identify opportunities for improvement.
WBH-FR-91	Change and Configuration Management	Controls related to change management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.
WBH-FR-92	Change and Configuration Management	The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.
WBH-FR-93	Change and Configuration Management	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.
WBH-FR-94	Change and Configuration Management	The Configuration Management Database (CMDB) shall be managed such that it ensures its reliability and accuracy including control of update access.
WBH-FR-95	Change and Configuration Management	The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.
WBH-FR-96	Change and Configuration Management	Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.

S. No.	Nature of Requirement	Minimum Requirement Specifications
WBH-FR-97	Change and Configuration Management	Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.
WBH-FR-98	Change and Configuration Management	A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.
WBH-FR-99	Change and Configuration Management	Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hardware configuration images.
WBH-FR-100	Change and Configuration Management	Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hardware configuration images.
WBH-FR-101	ICT Assets Hardening	All the ICT assets shall be hardened as per the Hardening guidelines and industry leading practices. Remove all unauthorized software, utilities, and services. All required logs shall be configured and monitored.

### 8.3 Disaster Recovery Infrastructure Software

Sr. No.	Minimum Requirement Description
1	The proposed solution must offer a workflow based management & monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts( including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices

6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, and Unix etc. with high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

## 9. Annexure II: IP Camera Locations

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
1.	Kichlu Chowk	Civil line Thana	Cross Road	Traffic Congestion Points	4	-	-	-	-	1	0
2.	Jaysingh Chowk	Civil line Thana	Chowk	Traffic Junctions	14	-	-	-	-	0	0
3.	Islamabad -T-Point to Gobindgarh Fort	Islamabad	T-Point	Traffic Congestion Points	4	-	-	-	-	0	0
4.	Katrabhai Sant Singh Chowk	D Div	T-Point	Crime Hotspot	2	-	2	-	-	0	1
5.	Mazjid Bazarsirki Bandar	D Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
6.	Shakti Nagar Chowk	D Div	T-Point	Traffic Junctions	14	-	-	-	3	1	0
7.	Majith Mandi Chowk	D Div	Circle	Crime Hotspot	14	-	-	-	-	1	0
8.	Chowk Chaursti Attari	C Div	T-Point	Crime Hotspot	2	3	0	-	-	0	1
9.	Jamadar Haweli	C Div	T-Point	Tourist Hotspot	9	-	-	-	3	0	0
10.	B.K E&I Sr.Sec School	D Div	One way	School	11	-	-	-	2	0	0
11.	B.K Dutt Gate	D Div	Cross Road	School	11	-	-	-	3	0	0
12.	Lahori gate	D Div	Circle	Traffic Junctions	14	-	-	1	-	0	0
13.	Khajana Gate	D Div	Circle	Traffic Congestion Points	4	-	-	-	4	0	0
14.	Balmik Mohalla	D Div	T-Point	Crime Hotspot	2	-	3	-	-	0	1
15.	Gate Hakima Main Chowk	Gate Hakima Thana	Circle	Traffic Junctions	14	-	-	-	3	0	0
16.	Main Road bangla basti	Gate Hakima Thana	Two Way	Crime Hotspot	2	2	-	-	-	0	1
17.	Pumme Di Pulli Near Bhadrakali	Gate Hakima Thana	Two Way	Tourist Hotspot	9	-	-	-	2	0	0
18.	Chabal Road mord gurbash nagar(Nr.Bhadrakali Mandir)	Gate Hakima Thana	Two Way	Traffic Congestion Points	4	-	-	-	4	0	0
19.	Chabal Road mord Gurbash	Gate Hakima Thana	Two Way	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
20.	Chabal Road Railway Crossing	Gate Hakima Thana	Two Way	Crime Hotspot	2	-	2	-	2	0	1
21.	T-Point Chabal Road	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
22.	Adda fatehpura	Gate Hakima Thana	T-Point	City Entry/Exit Points	5	-	-	-	4	1	4
23.	Amritsar Entrance Bridge Nr Gurudhwara(gate Hakima)	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
24.	T-Point Mord Fatehsingh Colony	Gate Hakima Thana	One way	Traffic Junctions	14	-	-	-	2	0	0
25.	Fatehsingh Colony Gali No:-22	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
26.	T-Point Fatehsingh Coloney Fatehpura Road	Gate Hakima Thana	T-Point	City Entry/Exit Points	5	-	-	-	4	1	4
27.	Amritsar Entrance	B Div	T-Point	City Entry/Exit Points	5	-	-	-	4	1	4
28.	Bhandari Bridge	Civil line Thana	Circle	Traffic Congestion Points	4	-	-	-	4	1	0
29.	Husanpura circle	A Div	Circle	Traffic Junctions	14	-	-	-	4	0	0
30.	Tandoor wala Chowk	A Div	Two Way	Traffic Junctions	14	-	-	-	5	0	0
31.	Sangam Chowk	A Div	Two Way	Traffic Junctions	14	-	-	-	4	1	0
32.	City Center Back Slde	A Div	Two way	Crime Hotspot	2	-	2	-	0	1	
33.	City Center Market Front Side	A Div	Two way	Traffic Junctions	14	-	-	-	2	1	0
34.	Surajchand Mansingh Gate	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
35.	Sherawala Gate	E Div	Circle	Traffic Junctions	14	-	-	-	3	0	0
36.	Ghee Mandi Akali Phula Singh	E Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
37.	Chita Gummat Chowk	A Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
38.	Ram Bagh	A Div	Circle	Crime Hotspot	2	-	2	-	0	1	
39.	Ram Talai	A Div	Cross Road	Crime Hotspot	2	-	2	-	0	1	

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
40.	Chimrang Road	B Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
41.	J.C Motor(100Ft Road)	B Div	Cross Road	Traffic Junctions	14	-	-	-	3	0	0
42.	Mata Kola Chowk	B Div	Two Way	Traffic Junctions	14	-	-	-	4	0	0
43.	Pratap Nagar Near OBC Bank	B Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
44.	Thind Dairy	B Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
45.	Tarawala Bridge	B Div	Circle	City Entry/Exit Points, Crime Hotspot	5, 2	-	-	-	4	1	0
46.	New Amritsar Gate	B Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
47.	Golden Gate	B Div	Two Way	Traffic Junctions	14	-	-	-	2	1	0
48.	Sultanwind chowk (Amritsar Entrance Village)	Sultanwind	Two Way	Crime Hotspot	2	-	2	-	0	1	
49.	Drama Wala bazar	B Div	Two Way	Markets	10	-	-	-	2	0	0
50.	Chora bazar	B Div	One Way	Markets	10	-	-	-	1	0	0
51.	Chungiwala bazar	B Div	One way	Markets, Crime Hotspot	10, 2	-	-	-	1	0	0
52.	Uttamnagar Ganda nala Sultanwind chowk	B Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
53.	Sultanwind Gate	B Div	Circle	Traffic Junctions	14	-	-	-	4	0	0
54.	Ajit Nagar Chowk(Dhingra	B Div	Circle	Traffic Junctions	14	-	-	]	4	0	0
55.	Hall Gate	E Div	Circle	Traffic Congestion Points	4	-	-	-	2	1	0
56.	Dana Mandi	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
57.	Jwala Mohan Floor Mill	Islamabad	Two Way	Traffic Junctions	14	-	-	-	2	0	0
58.	Bhagawala Chowk	Gate Hakima Thana	Circle	Crime Hotspot	2	-	2	-	0	1	
59.	Roop Nagar Main Road Near Lovely Chicken 1	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
60.	Roop Nagar Main Road Near Lovely Chicken 2	Gate Hakima Thana	T-Point	Traffic Junctions	14	-	-	-	2	0	0
61.	Shiv Gali	C Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
62.	Choti dhab bazar(Shivsanti	C Div	Two Way	market	10	-	-	-	2	0	0
63.	Sutto wala bazar	C Div	Chowk	market	10	-	-	-	3	0	0
64.	Guru Bazar chowk	E Div	Two Way	market	10	-	-	-	2	0	0
65.	Mahajan Kulfi Wala	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
66.	Goal Hatti Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
67.	RS Tower Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
68.	Shastri Market Dena Bank	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
69.	State Bank Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	4	0	0
70.	Amrita Talkie Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
71.	Ghee Mandi Mohalla	E Div	Five Way	Traffic Junctions	14	-	-	-	2	0	0
72.	T-Point Tahil Shaheb Bazar	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
73.	Guru Ravidas Road Hall Gate	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
74.	Kairon Market	E Div	T-Point	Traffic Congestion Points	4	-	-	-	2	0	0
75.	T-Point New Town Hall	E Div	Chowk	Traffic Junctions	14	-	-	-	2	0	0
76.	Arya School Lohgarh	E Div	T-Point	School	11	-	-	-	2	0	0
77.	Chowk Regent Cinema Lassiwala	E Div	Cross Road	Traffic Junctions	14	-	-	1	-	0	0
78.	Chowk Bharwan Ka Dhaba	E Div	Chowk	Traffic Junctions	14	-	-	-	2	0	0
79.	Chowk Katra Jaimal Singh	E Div	Chowk	Traffic Junctions	14	-	-	-	2	0	0
80.	Telephone Exchange	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
81.	Karmon Diodhi Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
82.	Turn Point Pratap bazar	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
83.	Katra Ahuwalia Chowk	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
84.	Turn Point Guru bazar	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
85.	DAV School both side Gate I/S	E Div	T-Point	School	11	-	-	-	2	0	0
86.	Subhash Juice Bar Sikndari Gate	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
87.	Kesar Da Dhaba	E Div	T-Point	Traffic Congestion Points	4	-	-	-	2	0	0
88.	Bombay Wala Kua	E Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
89.	Guruduara Lohgarh Sahib	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
90.	Outer Gate Busstand	A Div	Two Way	Bus stand	7	2	-	-	1	2	
91.	Purani Sabji Mandi	E Div	Two Way	Markets	10	-	-	-	2	0	0
92.	Chowk Farid Mathian Wala	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
93.	Chitra Taki Road	E Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
94.	DAV College Inside Both Outside	E Div	Cross Road	School	11	-	-	-	2	1	0
95.	Outside Ram Baug Church Road	A Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
96.	Katra Baghian Chowk	A Div	T-Point	Traffic Junctions	14	-	-	-	3	0	0
97.	Sabji Mandi samasan Ghat	Sultanwind	T-Point	Market	10	-	-	-	3	0	0
98.	Wallah Mandi Back Side	Mohkampura	Two Way	Traffic Junctions	14	-	-	1	-	0	0
99.	DAV International School Bypass	Verka	Y-Point	School	11	-	-	1	-	0	0
100.	Fatehgarh Sukur Chak Bypass	Verka	Cross Road	Traffic Junctions	14	-	-	-	4	0	0
101.	Gurudhwara Kotha Shaheb	Verka	Two Way	Traffic Junctions	14	-	-	-	2	0	0
102.	Verka Bus Stand	Verka	Two Way	Bus stand	7	2	-	-	4	0	2
103.	Chowk Bille wala Mohkampura	Mohkampura	Cross Road	Traffic Junctions	14	-	-	1	-	0	0
104.	Gururamdas Hostipital Vallah Gate	Verka	Two Way	City Entry/Exit Points	5	-	-	-	4	1	4

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
105.	Focal Point 1-2	Maqbulpura	T-Point	Government Infrastructure Assets	17	-	-	-	8	0	0
106.	Chowk Vallah	Verka	Y-Point	Traffic Junctions	14	-	-	-	4	1	0
107.	Chowk Milk Plant Verka	Verka	Circle Cross Road	Government Infrastructure Assets	17	-	-	1	-	0	0
108.	Preet Nagar sikha Gas Godown	Mohkampura	Two Way	Government Infrastructure Assets	17	-	-	-	0	0	0
109.	Opposite Apex Hostpital	Mohkampura	T-Point	Traffic Junctions	14	-	-	1	-	0	0
110.	Gurudhwara Wala Chowk		Chowk	Traffic Junctions	14	-	-	1	-	0	0
111.	Pawan Nagar Gali No:-5	Rambagh	Y-Point	Traffic Junctions	14	-	-	1	-	0	0
112.	Outside Jagat Jyoti School	Rambagh	Two Way	Traffic Junctions	14	-	-		2	0	0
113.	Chungiyani Chowk		T-Point	Traffic Junctions	14	-	-	1	-	0	0
114.	Suncity T-Point & Suncity Mord	Maqbulpura	Two Way	Traffic Junctions	14	-	-	1	-	0	0
115.	Chowk Mudal Bypass	Verka	Cross Road	City Entry/Exit Points	5	-	4	-	-	1	4
116.	Gurudhwara Wali Gali:14 Dashmesh Nagar	Mohkampura	Two Way	Traffic Junctions	14	-	-	1	-	0	0
117.	Chowk Judge Nagar(Nr.Gurudhwara Shahib	Mohkampura	T-Point	Traffic Junctions	14	-	-	-	2	0	0
118.	Domai Mandir	Mohkampura	Two Way	Temple	9	-	-	-	3	0	0
119.	Jora Fatak	Mohkampura	Y-Point	Crime Hotspot	2	-	5	-		0	1
120.	T-Point Ghanaiya Hostpital	A Div	T-Point	Hospital	13	-	-	-	0	0	0
121.	Matakola Balai Kendra Gali	E Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
122.	Outside Mission Compond	E Div	One Way	Traffic Junctions	14	-	-	-	1	0	0
123.	Galiyara Parking Chowk	E Div	Circle	Parking	14	-	-	-	2	1	0
124.	Shivala Virbhan	E Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
125.	T-Point Ramanand Bagh	E Div	T-Point	Traffic Junctions	14	-	-	1		0	0
126.	Islamabad T-point to govindgarh	Islamabad	T-Point	Tourist Hotspot	9	-	-	-	3	0	0
127.	Katra Karam Singh Chowk	D Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
128.	Purani Lakad Mandi Chowk	E Div	Circle	Traffic Junctions	14	-	-	1	-	0	0
129.	Chowk Chabutra	C Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
130.	Sharma Colony Near	C Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
131.	Tapai Fatak	Islamabad	Y-Point	Traffic Junctions	14	-	-	-	2	0	0
132.	Bakarmandi Chowk	Islamabad	T-Point	Traffic Junctions	14	-	-	1		0	0
133.	Chatiwind Chowk	C Div	Circle	Traffic Junctions	14	-	-	-	4	2	0
134.	Chatikhui Chowk	C Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
135.	Purani Chungi Teg Royal Hotel Tarang Taran Road	C Div	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
136.	Majivadiya Kabra	C Div	Y-Point	Traffic Junctions	14	-	-	-	2	0	0
137.	Mohni Chowk	Cantonment	Circle	Traffic Junctions	14	-	-	-	2	0	0
138.	Karori Chowk	C Div	Two Way	Traffic Junctions	14	-	-	-	2	0	0
139.	Baba Shahib Chowk	C Div	T-Point	Tourist Hotspots Entry/Exit Points	9	-	-	-	3	0	0
140.	Dholimala T-Point	C Div	T-Point	Crime Hotspot	2	-	3	-	3	0	1
141.	Ramsar Road Near Baba Deep Singh Gurudhwara	C Div	Cross Road	Tourist Hotspots Entry/Exit Points	9	-	-	-	2	0	0
142.	Laxmansar Chowk	C Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
143.	Chowk Gujjarpura	C Div	Chowk	Traffic Junctions	14	-	-	-	2	0	0
144.	Navacoat bazar Road	Islamabad	T-Point	Traffic Junctions	14	-	-	1		0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
145.	T-point Right Bridge Near CKD	Islamabad	T-Point	Traffic Junctions	14	-	-	1		0	0
146.	B-Block gate 1,2	Islamabad	One Way	Traffic Junctions	14	-	-	-	2	0	0
147.	Islamabad Chowk	Islamabad	Cross Road	Traffic Congestion Points	4	-	-	-	2	0	0
148.	Machi Mandi near Fatak	Islamabad	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
149.	Islamabad Bridge	Islamabad	T-Point	Traffic Junctions	14	-	-	1	-	0	0
150.	Soorchowk Balmiki Chowk	Cantonment	Circle	Traffic Junctions	14	-	-	1	-	0	0
151.	Putlighar Chowk	Cantonment	Cross Road	Crime Hotspot	2	2	-	-	-	1	1
152.	Kishan Kot Fatak	Islamabad	Two Way	Traffic Junctions	14	-	-	-	2	0	0
153.	Bhagta wala gate	Gate Hakima Thana	Circle	Traffic Junctions	14	-	-	-	2	0	0
154.	Galwali gate	C Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
155.	Kallu ka akhada	C Div	Circle	Traffic Junctions	14	-	-	-	2	0	0
156.	Naiya wala more	Islamabad	T-Point	Traffic Junctions	14	-	-	1		0	0
157.	Hotel Best western	Civil line Thana	T-Point	Market	10	-	-	-	2	1	0
158.	T-Point MK Hotel	Civil line Thana	T-Point	Market	10	-	-	-	2	0	0
159.	Amritsar Improvement trust	Civil line Thana	Cross Road	Traffic Junctions	14	-	-	-	1	0	0
160.	Ranjit Avenue Chowki	Civil line Thana	Chowk	Market	10	-	-	-	2	0	0
161.	C-Block Chowk Ranjit Avenue	Civil line Thana	Circle	Market	10	-	-	-	2	0	0
162.	Ranjit Avenue T-Point	Civil line Thana	T-Point	Traffic Junctions	14	-	-	1		0	0
163.	Purani Chungi	Civil line Thana	Circle	Traffic Junctions	14	-	-	1		0	0
164.	DC Kothi Green Avenue	Civil line Thana	T-Point	Traffic Junctions	14	-	-	1		0	0
165.	Incometax Chowk	Civil line Thana	Cross Road	Traffic Congestion Points	4	-	-	-	1	1	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
166.	Mall Cross Road	Civil line Thana	Cross Road	Traffic Congestion Points	4	-	-	-	1	0	0
167.	Novelty Chowk	Civil line Thana	Cross Road	Traffic Congestion Points	4	-	-	-	2	1	0
168.	Joshi Colony Chowk	Civil line Thana	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
169.	Garden Colony	Civil line Thana	T-Point	Traffic Junctions	14	-	-	1		0	0
170.	Jamunwali Road	Civil line Thana	T-Point	School	11	-	-	-	2	0	0
171.	B.R Modern School	Civil line Thana	Cross Road	School	11	-	-	-	2	0	0
172.	DAV Police Public School	Civil line Thana	Two Way	School	11	-	-	-	2	0	0
173.	Rani ka Bagh Near Gift Shop	Civil line Thana	Cross Road	Crime Hotspot	2	-	2	-		0	1
174.	Amandeep Hostpital	Civil line Thana	Y-Point	Hospital	13	-	-	-	0	0	0
175.	Mord Guru Arjan Dev Nagar	Cantonment	Two Way	Traffic Junctions	14	-	-	-	2	0	0
176.	Khalsa College Near Nikkasingh	Cantonment	Cross Road	School	11	-	-	-	2	1	0
177.	22 No Fatak	Islamabad	T-Point	Traffic Junctions	14	-	-	1	-	0	0
178.	Metro Bus Stand Near Khalsa	Cantonment	Cross Road	School	11	-	-	1	-	0	0
179.	Purani Chungi Chehrta Road	Chheharta	Cross Road	Traffic Junctions	14	-	-	-	4	1	0
180.	Khandwala Near Chehta Road	Chheharta	T-Point	Traffic Junctions	14	-	-	1	-	0	0
181.	Sandhu Colony	Chheharta	Cross Road	Traffic Junctions	14	-	-	1		0	0
182.	Kale Ka Mode Chehta Road	Chheharta	Two Way	Traffic Junctions	14	-	-	-	2	1	0
183.	Chehta Cross Road	Chheharta	Cross Road	Traffic Junctions	14	-	-	1		0	0
184.	Narayan Garh Chehta	Chheharta	Two Way	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
185.	India Gate Chehta Road	Chheharta	Cross Road	City Entry/Exit Points	5	-	-	-	3	1	4
186.	Wadali T-Point	Chheharta	T-Point	Traffic Junctions	14	-	-	-	3	0	0
187.	Sunsahab Gurudhwara	Chheharta	One Way	City Entry/Exit Points	5	-	-	-	4	1	2
188.	Kort Khalsa Chowk	Chheharta	T-Point	Traffic Junctions	14	-	-	-	3	0	0
189.	Nika Singh Coloney	Chheharta	Circle	Traffic Junctions	14	-	-	-	2	0	0
190.	Mahal PP	Cantonment	T-Point	City Entry/Exit Points	5	-	-	-	3	1	4
191.	Darshan Singh Ka Dera	Chheharta	Y-Point	Traffic Junctions	14	-	-	1		0	0
192.	Gawal Mandi Chowk	Cantonment	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
193.	Shimla Market	Cantonment	T-Point	Market	10	-	-	-	2	0	0
194.	Pipli Shab Gurudhwara	Islamabad	One Way	Traffic Junctions	14	-	-	-	2	0	0
195.	Parshuram Chowk	Cantonment	Circle	Traffic Junctions	14	-	-	1	-	0	0
196.	Bhandari Bridge To Goal Bagh(Pakode wala)	Civil line Thana	Y-Point	Traffic Junctions	14	-	-	-	2	0	0
197.	UCO Bank	Civil line Thana	Cross Road	Traffic Junctions	14	-	-	-	1	0	0
198.	Crystal Chowk	Civil line Thana	Cross Road	Traffic Congestion Points	4	-	-	-	2	1	0
199.	Coat Atmaram Road	Sultanwind	T-Point	Traffic Junctions	14	-	-	1	-	0	0
200.	Jaspal nagar DI Galiya	Sultanwind	T-Point	Traffic Junctions	14	-	-	1		0	0
201.	Tej Nagar Chowk	Sultanwind	Chowk	Traffic Junctions	14	-	-	-	2	0	0
202.	Sharah Baba Deepsingh ji Shidhwala	Sultanwind	T-Point	City Entry/Exit Points	5	-	-	-	3	1	4
203.	Chowk Tandan Nagar	Rambagh	T-Point	Traffic Junctions	14	-	-	1		0	0
204.	Murgikhan Wali Gali	Mohkampura	Two way	Traffic Junctions	14	-	-	-	2	0	0
205.	Banke bihari Wali Gali	Mohkampura	Two way	Traffic Junctions	14	-	-	1		0	0
206.	Baba Meer Shah Nehru Colony	Sadar	T-Point	Traffic Junctions	14	-	-	-	3	0	0
207.	Papa public school, 88 feet road	Sadar	Two way	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
208.	27ft Road Green Field Road	Sadar	Two way	Traffic Junctions	14	-	-	-	2	0	0
209.	Tungawali Gali(ESI Road)	Sadar	Circle	Traffic Congestion Points	4	-	-	-	2	0	0
210.	Borh wala shivala batala road	Sadar	T-Point	Traffic Congestion Points	4	-	-	-	2	0	0
211.	Mai bhago college majitha road	Sadar	Two way	Traffic Junctions	14	-	-	-	3	1	0
212.	D.R enclave	Airport Thana	Two way	Traffic Junctions	14	-	-	-	2	0	0
213.	Loharka chowk bridge	Cantonment	Y-Point	Traffic Junctions	14	-	-	-	2	0	0
214.	Meera kot chowk	Cantonment	cross road	Traffic Junctions	14	-	-	1	1	1	0
215.	Ekam dhaba g.t road	Airport Thana	Two way	Traffic Junctions	14	-	-	-	2	0	0
216.	Pind heir	Airport Thana	Two way	Traffic Junctions	14	-	-	-	2	0	0
217.	Gumtala bypass chowk	Cantonment	cross road	Traffic Congestion Points	4	-	-	-	2	1	0
218.	T point airport road	Airport Thana	T-Point	Airport Entry / Exit Points	8	-	-	-	3	1	4
219.	Akash amar Chowk Fateh garh Chudiya Road	Sadar	T-Point	Traffic Junctions	14	-	-	1		0	0
220.	Ajay Sr.Secondary School (Amar Jyoti School)Sakhe Di Haweli	Sadar	T-Point	Traffic Junctions	14	-	-	-	2	0	0
221.	Fatehgarh Bypass Chowk	Sadar	Chowk	Traffic Junctions	14	-	-	-	1	0	0
222.	Baba Deep Singh Coloney-	Sadar	T-Point	Traffic Junctions	14	-	-	1		0	0
223.	Majitha Chowk Bypass	Sadar	Cross Road	City Entry/Exit Points	5	-	-	-	4	1	4
224.	Govt High school near park pani wali tenka friends colony	Sadar	Two way	Traffic Junctions	14	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
225.	Mustafa chowk	Sadar	T-Point	Traffic Congestion Points	4	-	-	-	2	0	0
226.	Civilline T-Point Near Namthari Gurudhwara	Civil line Thana	Y-Point	Traffic Junctions	14	-	-	1		0	0
227.	Hukumsingh Road	Civil line Thana	Y-Point	Traffic Junctions	14	-	-	1		0	0
228.	Company Baug	Civil line Thana	Two way	Traffic Junctions	14	-	-	-	2	0	0
229.	Congress bhavan, Near Circuit House	Civil line Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
230.	Doaba Chowk	Civil line Thana	T-Point	Traffic Junctions	14	-	-	-	3	0	0
231.	Daily Needs	Cantonment	Two way	Traffic Junctions	14	-	-	-	2	0	0
232.	Saroop rani govt college	Civil line Thana	Two way	Colleges	12	-	-	-	2	0	0
233.	Commissioner of police, amritsar	Civil line Thana	Two way	Administrative Building	16	-	-	-	2	0	0
234.	Govt senior secondary school,	Civil line Thana	Two Way	school	11	-	-	-	2	0	0
235.	Guru Arjun Dev Nagar Mod	Cantonment	Chowk	Traffic Junctions	14	-	-	-	2	0	0
236.	Gopal Mandir Chowk	Sadar	Chowk	Traffic Junctions	14	-	-	-	3	1	0
237.	Amritsar Toll Plaza, Manawala, ANPR	Rural ASR	Two way	City Entry/Exit Points	5	-	-	-	4	1	2
238.	Amritnal Bagh (Rose Garden)	Civil line Thana	Entry/Exit	Park	3	-	-	-	2	0	0
239.	Prakash Hospital	Cantonment	Entry/Exit	Hospital	13	-	-	-	0	0	0
240.	Jaliawala Baug	C Div	Two way	Traffic Junctions	14	-	-	-	2	0	0
241.	Beri hospital	Cantonment	T-Point	Hospital	13	-	-	-	0	0	0
242.	Navpreet Hospital	Cantonment	Entry/Exit	Hospital	13	-	-	-	0	0	0
243.	Carewell Hospital		Entry/Exit	Hospital	13	-	-	-	0	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
244.	S.Raminder Singh Bulariya Park	C Div	Entry/Exit	Park	3	-	-	-	3	1	0
245.	Green avenue park(Nr verka booth)	Civil line Thana	T-Point	Traffic Congestion Points	4	-	-	-	3	1	0
246.	Park Guru Govind singh Nagar	Cantonment	Two way	Park	3	-	-	-	2	0	0
247.	Amritbakery Opp-Kabir Park	Cantonment	Cross Road	Traffic Junctions	14	-	-	-	2	0	0
248.	Kabir Park Market Opp-GNDU	Cantonment	Cross Road	Traffic Junctions	14	-	-	-	2	1	0
249.	Shivaji Park, Rani ka Bagh	Civil line Thana	T-Point	Traffic Junctions	14	-	-	-	3	1	0
250.	Katra Moti Ram park Near Soyabin Wali Dukan	D Div	Two Way	Traffic Junctions	14	-	-	-	3	1	0
251.	Park Beri gate	D Div	Cross Road	Traffic Junctions	14	-	-	-	2	1	0
252.	Vijaynagar, Kashmir Avenue, Back side Krishna Sweets	A Div	Park	Procession/Gathering Hotspots	3	-	-	-	3	1	0
253.	Shivala Colony	A Div	Park	Procession/Gathering Hotspots	3	-	-	-	4	1	0
254.	Krishna Square, Water tank Park	A Div	Park	Procession/Gathering Hotspots	3	-	-	-	3	1	0
255.	Dumb School, Tehsilpura	A Div	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
256.	40 Kuh main park	Mohkampura	Park	Procession/Gathering Hotspots	3	-	-	-	5	1	0
257.	Golden Avenue, Near Veer Heekikat Rai	Maqbulpura	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
258.	Focal point Opp Police Station	Maqbulpura	Police station	Procession/Gathering Hotspots	3	-	-	-	3	1	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
259.	Baba Deep Singh Nagar	Sultanwind	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
260.	Veer Enclave, Opp Riyani Public School	Rural ASR	Park	Procession/Gathering Hotspots	3	-	-	-	4	1	0
261.	Hindu Sabha, Sr Secondary School	D Div	School	Procession/Gathering Hotspots	3	-	-	-	2	1	0
262.	Park Shakti Nagar	D Div	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
263.	Subhash Park, Katra Sher Singh	E Div	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
264.	Town Hall	E Div	Park	Procession/Gathering Hotspots	3	-	-	-	3	1	0
265.	Ucha Park, Near Godam Mohalla	E Div	Park	Procession/Gathering Hotspots	3	-	-	-	3	1	0
266.	Govt Sr Secondary School Gate, GT Road, Putiligarh	Cantonment	School	Procession/Gathering Hotspots	3	-	-	-	2	1	0
267.	Dhobi Ghat, Near Gate Hariman Chowk	Gate Hakima Thana	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
268.	Friends Colony, Opp Harimandir Majitha Road	Sadar	Park	Procession/Gathering Hotspots	3	-	-	1	-	1	0
269.	Joshi Colony Park	Civil line Thana	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
270.	Park Pani wali Tanki, Near Japani Mill	Chheharta	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
271.	Triconi Park, Rani ka bagh	Civil line Thana	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
272.	Gurudwara Singh Sabha, Opp Rani Ka Bagh	Civil line Thana	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
273.	Goal Bagh	Civil line Thana	Park	Procession/Gathering Hotspots	3	-	-	-	2	1	0
274.	Arya Samaj School Park		Park Area	Park	3	-	-	-	2	1	0
275.	Open Space_Sewa Kendra_Opp Arya Samaj School Park		Park Area	Park	3	-	-	-	2	1	0
276.	Peripheral Park		Park Area	Park	3			-	6	1	0
277.	Gang Di Mori Park		Park Area	Park	2		2	-		1	1
278.	Sant Nagar Park Dolphin Park		Park Area	Park	3		-	-	2	1	0
279.	Gali Munshiyan Rodanwali		Park Area	Park	3		-	-	2	1	0
280.	Gali Hargobindpura	Chheharta	Park Area	Park	3		-	-	2	1	0
281.	Chhattiwind Nehar	Sultanwind	Entry/Exit	City Entry/Exit	5		-	-	4	1	2
282.	District HQ, Amritsar	Civil line Thana	Office Entry	Administrative Building	16	-	-	-	2	0	0
283.	Iswar nagar Chawk	C Div	T-Point	Traffic Junctions	14	-	-	1	-	0	0
284.	Guru Amar Das Nagar Chawk	C Div	Cross Road	Traffic Junctions	14	-	-	1	-	0	0
285.	Bagchi Iakha Singh Chawk	C Div	Cross Road	Traffic Junctions	14	-	-	1	-	0	0
286.	District Shoping Complex Parking	Civil line Thana	Market and Parking	Main Markets Entry	10	-	-	-	6	0	0
287.	Rashtriya Bal School Islamabad	Islamabad	School	Schools	11	-	-	-	2	0	0
288.	Model School Islamabad	Islamabad	School	Schools	11	-	-	-	2	0	0
289.	RBBSK Primary School	Islamabad	School	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
290.	Atom Public School Islamabad Chaatwali Gali	Islamabad	School	Schools	11	-	-	-	2	0	0
291.	Apex International School, Rani ka Bagh	Civil line Thana	School	Schools	11	-	-	-	2	0	0
292.	NavBharat School 33 Number	Cantonment	School	Schools	11	-	-	1		0	0
293.	Khalsa College Women	Cantonment	College	Government Colleges	12	-	-	-	2	0	0
294.	Khalsa College	Cantonment	College	Government Colleges	12	-	-	-	2	0	0
295.	Khalsa School	Cantonment	School	Schools	11	-	-	-	2	0	0
296.	GND University	Cantonment	College	Government Colleges	12	-	-	-	3	0	0
297.	Twinkle Star School Guru Nanak	Islamabad	School	Schools	11	-	-	-	2	0	0
298.	Bhavan SI Public School 33	Sadar	School	Schools	11	-	-	-	2	0	0
299.	Ranjit Avenue ITI College	Civil line Thana	College	Colleges	12	-	-	-	3	0	0
300.	Guru Ram Das Dental College 100 Ft Road	B Div	College	Colleges	12	-	-	-	2	0	0
301.	SSSS School	Civil line Thana	School	Schools	11	-	-	-	2	0	0
302.	Ram Ashram School	Civil line Thana	School	Schools	11	-	-	-	2	0	0
303.	Police DAV School Lawrence	Civil line Thana	School	Schools	11	-	-	-	2	0	0
304.	Guru Har Krishan Public School or CKD College GT Road	Civil line Thana	School	Schools	12	-	-	-	2	0	0
305.	Holi Heart School GT Road	Cantonment	School	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
306.	Prem Ashram School, Beri gate Market	D Div	School	Schools	11	-	-	-	2	0	0
307.	Hindu Sabha School	D Div	School	Schools	11	-	-	-	2	0	0
308.	Prakash Ashram School, Inside Hatti Gate	E Div	School	Schools	11	-	-	-	2	0	0
309.	Mental Hospital	Sadar	Hospital	Hospital	13	-	-	-	0	0	0
310.	Beri Hospital	Cantonment	Hospital	Hospital	13	-	-	-	0	0	0
311.	Navpreet Hospital	Cantonment	Hospital	Hospital	13	-	-	-	0	0	0
312.	Ohri Hospital	Cantonment	Hospital	Hospital	13	-	-	-	0	0	0
313.	Care and Cure Hospital	Civil line Thana	Hospital	Hospital	13	-	-	-	0	0	0
314.	Soor Hospital Khajana Gate	D Div	Hospital	Hospital	13	-	-	-	0	0	0
315.	Mahajan Hospital	D Div	Hospital	Hospital	13	-	-	-	0	0	0
316.	Narang Hospital	Islamabad	Hospital	Hospital	13	-	-	-	0	0	0
317.	Pasricha Hospital	Islamabad	Hospital	Hospital	13	-	-	-	0	0	0
318.	Bhatia Hospital	C Div	College	Colleges	13	-	-	-	0	0	0
319.	Khalsa College Ranjit Avenue	Civil line Thana	School	Schools	12	-	-	-	2	0	0
320.	Bedi School	Civil line Thana	College	Colleges	11	-	-	-	3	0	0
321.	Shehzada Nand College Green	Civil line Thana	College	Colleges	12	-	-	-	2	0	0
322.	BBK DAV International School	Civil line Thana	School	Schools	11	-	-	-	2	0	0
323.	Ryan International	B Div	School	Schools	11	-	-	-	2	0	0
324.	DPS School	Rural ASR	School	Schools	11	-	-	-	2	0	0
325.	Sant Kabir Public School Mandar Val Bazaar	B Div	School	Schools	11	-	-	-	2	0	0
326.	Ajit Vidhyalaya School Sultwind	B Div	School	Schools	11	-	-	-	2	0	0
327.	Shahed Baba Pratap Singh	B Div	School	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
328.	Saint Joseph School Rani ka	Civil line Thana	School	Schools	11	-	-	-	2	0	0
329.	Saint Joseph School Fatahpur	Gate Hakima Thana	School	Schools	11	-	-	-	2	0	0
330.	Cambridge School Loharka Road	Cantonment	School	Schools	11	-	-	-	3	0	0
331.	Pink Plaza	E Div	market	Main Markets Entry	10	-	-	-	2	0	0
332.	Meeri Peeri School	Chheharta	School	Schools	11	-	-	-	2	0	0
333.	Sacred Heart School Chungi	Sadar	School	Schools	11	-	-	-	2	0	0
334.	SM High Scholl Vikas Nagar	Chheharta	School	Schools	11	-	-	-	2	0	0
335.	DD High School Gobind Pura	Chheharta	School	Schools	11	-	-	-	2	0	0
336.	Narangarh Govt School Chehtra	Chheharta	School	Schools	11	-	-	-	2	0	0
337.	Medcrad Hospital Tran Taran	C Div	Hospital	hospital	16	-	-	-	0	0	0
338.	Govt School Nava Kot	Islamabad	School	Schools	11	-	-	-	2	0	0
339.	Amar School Nava Kot	Islamabad	School	Schools	11	-	-	-	2	0	0
340.	Twinkle Star School Navakot	Islamabad	School	Schools	11	-	-	-	2	0	0
341.	Guru Nanak Dev Hospital	Civil line Thana	Hospital	Government Hospital	13	-	-	-	0	0	0
342.	Hare Krishna Public School Majitha Road Bypass	Sadar	School	Schools	11	-	-	-	2	0	0
343.	Spring Dale School	Sadar	School	Schools	11	-	-	-	2	0	0
344.	Savan School Devi Nagar Fatehgarh Churian Road	Sadar	School	Schools	11	-	-	-	2	0	0
345.	Shiv Deep Public School New Nehru Colony	Sadar	School	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
346.	JK Public School Tung bala	Sadar	School	Schools	11	-	-	-	2	0	0
347.	Govt Public Tung Bala	Sadar	School	Schools	11	-	-	-	2	0	0
348.	Model Study School Tung Bala Majitha Road	Sadar	School	Schools	11	-	-	-	2	0	0
349.	Govt Sr Secondary School	Islamabad	School	Schools	11	-	-	-	2	0	0
350.	Preet Public School Mustafabad	Sadar	School	Schools	11	-	-	-	2	0	0
351.	SS High School Tungbala Guru Gobind Sing Nagar	Sadar	School	Schools	11	-	-	-	2	0	0
352.	Shivam Public School New	Sadar	School	Schools	11	-	-	-	2	0	0
353.	Saranagdhar Sr Secondary		School	Schools	11	-	-	-	2	0	0
354.	MahaShakti Vidhyabhawan Jawahar Road	Civil line Thana	School	Schools	11	-	-	-	2	0	0
355.	Bekish Shiksha Modern School Vijay Nagar	Sadar	School	Schools	11	-	-	-	2	0	0
356.	Bright Way Public School	Chheharta	School	Schools	11	-	-	-	2	0	0
357.	Roaming Angels Public School		School	Schools	11	-	-	-	2	0	0
358.	Punjab High School Gali no 1		School	Schools	11	-	-	-	2	0	0
359.	Tagore Modern School	E Div	School	Schools	11	-	-	-	2	0	0
360.	Sham Public School Gali 3 Indra Colony Mustafabad	Sadar	School	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
361.	Sunveli School Gopal Nagar Tower vali Gali	Sadar	School	Schools	11	-	-	1		0	0
362.	GD Goenika School	Cantonment	School	Schools	11	-	-	-	2	0	0
363.	CLH School Islamabad Dargah	Islamabad	School	Schools	11	-	-	-	2	0	0
364.	CLH School Putligarh	Cantonment	School	Schools	11	-	-	-	2	0	0
365.	Ajanta Public School	Civil line Thana	School	Schools	11	-	-	-	2	0	0
366.	Parvati Devi Hospital	Civil line Thana	Hospital	Hospital	13	-	-	-	0	0	0
367.	Hartej Hospital	Civil line Thana	hospital	hospital	13	-	-	-	0	0	0
368.	Kamal Mahajan Hathi Gate	E Div	Market	Crime Hotspot	2	-	2	-		0	1
369.	Saren Hospital	Sadar	Hospital	hospital	13	-	-	-	0	0	0
370.	Randhwara Health Care Center Karta Moti Ram Hathi Gate	E Div	Hospital	hospital	13	-	-	-	0	0	0
371.	Adlakha Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
372.	Amandeep Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
373.	Uppal Neuro Hospital Rani ka	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
374.	Ved Gupta Mall Road	Civil line Thana	market	Main Markets Entry	10	-	-	-		0	0
375.	Gurupreet Hospital 100 ft Road	B Div	Hospital	hospital	13	-	-	-	0	0	0
376.	EMC Hospital Green Avenue	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
377.	Dr. Diljit Singh Eye Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
378.	TB Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
379.	KD Hospital Circluar Road	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
380.	Sukh Sagar Hospital Basant	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
381.	Govt Medical College Majitha Road Medical Avenue	Civil line Thana	Hospital	hospital	13	-	-	-	2	0	0
382.	Chikitsa ENT Hospital Pink Plaza	E Div	Hospital	hospital	13	-	-	-	2	0	0
383.	Apollo Hospital Liberty	B Div	Hospital	hospital	13	-	-	-	0	0	0
384.	Kalra Hospital Sultan Wind Road	B Div	Hospital	hospital	13	-	-	-	0	0	0
385.	Swift Hospital	Sadar	Hospital	hospital	13	-	-	-	0	0	0
386.	Vidya Sagar Mental Hospital, Nirankari Colony	Civil line Thana	Hospital Gate	hospital	13	-	-	-	0	0	0
387.	Institute Of Mental Hospital, Circular Road, Nirankari Colony	Civil line Thana	Hospital Gate	hospital	13	-	-	-	0	0	0
388.	Government Mental Hospital, Circular Road	Civil line Thana	Hospital Gate	hospital	13	-	-	-	0	0	0
389.	Simran Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
390.	Ajit Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
391.	Anand Hospital and Heart	C Div	Hospital	hospital	13	-	-	-	0	0	0
392.	Randhawa Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0
393.	Harpreet Hospital	Civil line Thana	Hospital	hospital	13	-	-	-	0	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
394.	Idh Hospital		Hospital	hospital	13	-	-	-	0	0	0
395.	Machhi Mandi Market	E Div	Market	Main Markets Entry	10	-	-	-	2	1	0
396.	Shimla Market	Cantonment	Market	Main Markets Entry	10	-	-	-	2	1	0
397.	Alpha One Mall	Maqbulpura	Mall	Main Markets Entry	10	-	-	-	3	1	0
398.	Trillium Mall	Majitha Road PS	Mall	Main Markets Entry	10	-	-	1	-	1	0
399.	Celebration Mall	A Div	Market	Main Markets Entry	10	-	-	-	3	1	0
400.	Sultan Wind Clothes Market	B Div	Market	Main Markets Entry	10	-	-	-	3	1	0
401.	Bhadar Kalimandir Khajan Gate	Gate Hakima Thana	Market	Main Markets Entry	10	-	-	-	3	1	0
402.	Model Twon Mandir	Civil line Thana	Market	Main Markets Entry	10	-	-	-	3	1	0
403.	Company Bagh	Civil line Thana	Market	Main Markets Entry	10	-	-	-	2	3	0
404.	Gurunanak Stadium	Civil line Thana	Market	Main Markets Entry	10	-	-	-	2	1	0
405.	Beri Gate Market Pal Vala Area	D Div	Market	Main Markets Entry	10	-	-	-	2	1	0
406.	Putligarh Market Area	Cantonment	Market	Main Markets Entry	10	-	-	-	2	1	0
407.	Puda Bhawan	Civil line Thana	Government Office	Administrative Building	16	-	-	-	2	0	0
408.	Guru Nanak Nagar, Street No. 1	Islamabad	Cross Road	Traffic Junctions	14	-	-	-	4	1	0
409.	Chotta Haripur Chawk	Islamabad	Cross Road	Traffic Junctions	14	-	-	-	4	1	0
410.	Amritsar Bus stand	A Div	Bus Stand	Bus Stations Entry/Exit Points	7	6	-	-		3	2
411.	Mahakali Nav Greh Mandir , Sashtri Nagar	Civil line Thana	T-Point	Traffic Junctions	14	-	-	1	-	0	0
412.	General & Textile Union	Cantonment	Office Entry	Administrative Building	16	-	-	-	2	0	0
413.	Suvidha Centre (North	Civil line Thana	Cross Road	Govt Assets	17	-	-	1		0	0
414.	IKGPTU Campus Amritsar	Chheharta	College Gate	Colleges	12	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
415.	Central Institute of Plastics Engineering and Technology	Chheharta	College Gate	Colleges	12	-	-	-	2	0	0
416.	Bibek Academy School	Sultanwind	School Gate	Schools	11	-	-	-	2	0	0
417.	Govt. Sen. Sec School, Dhapai	Islamabad	School Gate	Schools	11	-	-	-	2	0	0
418.	Government Girls Senior Secondary School, Sundar Gali Bahadur Nagar, Katra Ahluwalia	E Div	School Gate	Schools	11	-	-	-	2	0	0
419.	Govt Girls Higher Secondary School, M S Gate, Shivala Road Katra Bhagian, Hall Bazar,	E Div	School Gate	Schools	11	-	-	-	2	0	0
420.	Govt high school, Rajinder Nagar Gali Number 3 Prem Nagar	Sadar	School Gate	Schools	11	-	-	-	2	0	0
421.	Government Middle School Railway B Block	Islamabad	School Gate	Schools	11	-	-	-	2	0	0
422.	Government Senior Secondary School, GT Road Naraingarh, Azad Nagar	Chheharta	School Gate	Schools	11	-	-	-	2	0	0
423.	Government High School, Karampura, E-Block	Civil line Thana	School Gate	Schools	11	-	-	-	2	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
424.	Govt. High School, Kala Pind,	Chheharta	School Gate	Schools	11	-	-	-	2	0	0
425.	Government Girls High School, M.C.Market, Bhagta Wala Gate	C Div	School Gate	Schools	11	-	-	-	2	0	0
426.	Government Saragarhi Memorial Secondary School	C Div	School Gate	Schools	11	-	-	-	2	0	0
427.	Government Saragarhi Memorial Secondary School, High School	C Div	school Gate	Schools	11	-	-	-	2	0	0
428.	Sarkari Secondary School, Katda Hakima, Outside Hakima Gate	Gate Hakima Thana	School Gate	Schools	11	-	-	-	2	0	0
429.	Vishav Public High School, Batala Rd, Guru Nanak Nagar	Sadar	School Gate	Schools	11	-	-	-	2	0	0
430.	Indian Institute of Management,	Chheharta	College Gate	Colleges	12	-	-	-	2	0	
431.	Vallah Mandi Area	Mohkampura	Market	Main Markets Entry	10	-	-	-	5	3	0
432.	Civil Hospital	A Div	Hospital	Administrative Building	13	-	-	-	4	1	0
433.	Basant Avenue Market	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
434.	Reyato chowk	Civil line Thana	Traffic Junctions	Traffic Congestion Points	4	-	-	-	0	0	0
435.	lawrence cross road	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
436.	DAV college / larence road	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
437.	Dausanda singh chowk	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
438.	Trillium mall junction	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
439.	Ratan singh chowk	Majitha Road PS	Traffic Junctions	Traffic Congestion Points	4	-	-	-	0	0	0
440.	ESI cross road	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
441.	88 ft Road entry	Sadar	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
442.	88FT exit	Sadar	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
443.	Kabir marg	Sadar	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
444.	Verka bypass	Sadar	Traffic Junctions	Traffic Congestion Points	4	-	-	-	0	0	0
445.	Makhan Restaurant chowk	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
446.	SSSS chowk	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
447.	Joshi colony market	Majitha Road PS	Traffic Junctions	Traffic Congestion Points	4	-	-	-	0	0	0
448.	Circular road (opposite TSPCL)	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
449.	Musta chowk (Bagh chowk)	Sadar	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
450.	Gala Mala marg	Majitha Road PS	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
451.	District shopping centre	Civil line Thana	Traffic Junctions	Traffic Congestion Points	4	-	-	-	0	0	0
452.	C Block market	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
453.	Green Avenue market	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
454.	Amrit nal bagh	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
455.	Railway station entry point	Civil line Thana	Traffic Junctions	Railway Stations Entry/Exit	6	1	-	-	0	0	1
456.	Railway station exit point	Civil line Thana	Traffic Junctions	Railway Stations Entry/Exit	6	1	-	-	0	0	1
457.	Railway station entry / exit, B/H	Civil line Thana	Traffic Junctions	Railway Stations Entry/Exit	6	2	-	-	0	0	2
458.	Durgiyana mandir (Hathi chowk)	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
459.	Durgiyana New Entrance	Civil line Thana	Traffic Junctions	Traffic Junctions	14	-	-	-	0	0	0
460.	Sultan Wind 100 feet road	B Div	Traffic Junctions	Traffic Junctions	14	-	-	-	3	1	0
461.	Gurunam nagar	Sultanwind	Traffic Junctions	Traffic Junctions	14	-	-	-	2	1	0
462.	100 Feet Sowadi Road	B Div	Crime Hotspot	Crime Hotspot	14	-	-	-	4	1	0
463.	Sunena Bazar, Guru Bazar	e Div	Crime Hotspot	Crime Hotspot	14	-	-	-	2	1	0
464.	Sheeda Sahib Gurudwara, ANPR	Chheharta	Crime Hotspot	Crime Hotspot	14	-	-	-	2	1	0
465.	Jahazgarh, ANPR	B Div	Crime Hotspot	Crime Hotspot	14	-	-	-	2	1	0
466.	Transport nagar	B Div	Crime Hotspot	Crime Hotspot	3	-	-	-	2	1	0
467.	Shastri Nagar, Park Lawrence Road	Civil line Thana	Park	Park	3	-	-	1	-	0	0
468.	Park Canady Avenue	Civil line Thana	Park	Park	3	-	-	1	-	0	0
469.	Dump Dump School, Tehsilpura	A Div	Park	Park	3	-	-	1	-	0	0
470.	Kashmir Avenue, Rose Garden	A Div	Park	Park	3	-	-	1	-	0	0
471.	Dhingra Complex, Near Panj Peer, G.T. Road	Mohkampura	Park	Park	3	-	-	1	-	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
472.	Park Chamrang Road, B/S Mata Kauhal Hospital	B Div	Park	Park	3	-	-	1	-	0	0
473.	Sakatri Bagh	C Div	Park	Park	3	-	-	1	-	0	0
474.	Hindu Shaba Sen. Sec. School, Amritsar	D Div	Park	Park	3	-	-	1	-	0	0
475.	Shubash Park, Katra Sher Singh	E Div	Park	Park	3	-	-	1	-	0	0
476.	Gurbkash Nagar, Green Park, Near Police Chownki,	Islamabad	Park	Park	3	-	-	1	-	0	0
477.	Mahadev Vidiya Niketan School, A-Block, Ranjit Avenue	Civil line Thana	Park	Park	3	-	-	1	-	0	0
478.	Bent Park, Opp MK Hotel	Civil line Thana	Park	Park	3	-	-	1	-	0	0
479.	Golbagh	Civil line Thana	Park	Park	3	-	-	1	-	0	0
480.	Moon Avenue, Sharma Park	Sadar	Park	Park	3	-	-	1	-	0	0
481.	Akash Avenue, Near DhamMandir Near Byepass	Sadar	Park	Park	3	-	-	1	-	0	0
482.	Trikoni Park, Rani ka Bagh	Cantonment	Park	Park	3	-	-	1	-	0	0
483.	Guruduara Singh Sahib, Rani Ka Bagh, opp. Park	Cantonment	Park	Park	3	-	-	1	-	0	0
484.	Government High School, Gate Hakima	Gate Hakima Thana	Park	Park	3	-	-	1	-	0	0
485.	B-Block, Railway Colony Park	Islamabad	Park	Park	3	-	-	1	-	0	0
486.	Green Avenue market		Park	Park	3	-	-	1	-	0	0

S. No.	Location Name	Police Station name	Type of Location	Location Name	Priority of Location	Indoor FRS	Outdoor FRS	Panoramic 360° Camera	Fixed Box Camera (GF)	PTZ Camera	ANPR
487.	Park Basant Avenue	Majitha Road PS	Park	Park	3	-	-	1	-	0	0
488.	Tripti Bala ji Mandir, Green field, Majitha Road	Sadar	Park	Park	3	-	-	1	-	0	0
489.	Gopal Nagar Near Hari Mandir, Tanki wali Gali, Majitha Road	Sadar	Park	Park	3	-	-	1	-	0	0
490.	Joshi colony	Civil line Thana	Park	Park	3	-	-	1	-	0	0
491.	Park Wali tanki, Near Japani Mills, Main Road Chheharta	Chheharta	Park	Park	3	-	-	1	-	0	0
492.	Shiva Ji Park, Rani ka Bagh	Cantonment	Park	Park	3	-	-	1	-	0	0
PTZ for Public Address System					-	-	-	-	-	25	0
	Total					21	35	75	778	130	72

## 10. Annexure III: Air Quality Monitoring Station Locations

S. No	Location Details	Environment Sensor
1.	Batala Road - Old Focal Point	1
2.	Ranjit Avenue Oarket	1
3.	Amritsar Bus Stand	1
4.	Sultan Wind Clothes Market	1
5.	East Mohan Nagar	1
6.	Tarn Taran Road	1

## 11. Annexure IV: Water Quality Analyzer

S. No	Location Details	Environment Sensor
1.	Tung Dhab Drain	1
2.	City Outfall Drain	1

## 12. Annexure V: Manpower Requirements

### 12.1 Manpower/Resource Requirements for Operations & Maintenance of Smart Solutions in Amritsar City

S. No.	Role	Quantity
1.	Project Manager - IT Infrastructure	1
2.	Technical Lead - IT Infrastructure	1
3.	System Admin - L2	1
4.	Network Admin - L2	1
5.	Security Specialist - L2	1
6.	DB Administrator - L2	1
7.	Video Analyst / IP Camera Surveillance Expert - L3	1
8.	Software Developer (Full Stack Developer) - L3	1
9.	Support Engineer - L1	1
10.	Electrical Maintenance Technician	1
11.	HVAC Technician	1
12.	EMS Engineer - L2	1
13.	BMS Engineer - L2	1
14.	Security Staff	1
15.	Help Desk - L1	1

#### 12.1.1 Project Manager - IT Infrastructure

S. No.	Description
1.	B.E. or B. Tech. with MBA or equivalent / M.E. or M.Tech / MCA or higher degree from a recognised university
2.	Should have experience of working in Government sector with minimum of 2 of large IT infrastructure / Data Centre / Smart City Solutions / Surveillance projects of similar scale.
3.	Should possess Industry accredited certifications like PMP/Prince 2 certified
4.	Minimum 15 years of experience in IT infrastructure out of which at least 8 years in / Data Centre / Smart City Solutions / Surveillance
5.	Should have minimum of two years of experience within the organization
6.	Responsible for the overall Contract performance and should not serve in any other capacity under this Contract
7.	Knowledge of organizing, planning, directing and coordinating the overall responsibilities
8.	Knowledge of the principles and methodologies associated with program management and expert in use of program management tools like Microsoft Project

*Note: It is presumed that Project Manager has considerable and reasonable executing powers to take informed decisions for smooth delivery of the Project*

### 12.1.2 Technical Lead

S. No.	Description
1.	B.E. or B. Tech. with MBA or equivalent / M.E. or M.Tech / MCA or higher degree from a recognised university
2.	Should have experience of working in Government sector as Technical lead in minimum 2 project in IT infrastructure / Data Centre / Smart City Solutions / Surveillance
3.	Industry accredited certifications like MCSE,MSCD,CCNA or certifications from OEM products
4.	Minimum 10 years of experience in IT infrastructure out of which at least 5 years in Data Centre / Smart City Solutions / Surveillance projects
5.	Should have minimum of two years of experience within the organization
6.	Should be PMP/Prince 2 certified
7.	Should not serve in any other capacity under this Contract

### 12.1.3 System Admin - L2

S. No.	Description
1.	B.E./B. Tech./MCA or higher degree from a recognized university
2.	Microsoft Certification (MCSE) , RHCE or similar certifications in System Administration tools/platforms/OS specifically used in this project
3.	Minimum 6 years of IT experience out of which 3 years as System Administrator in large scale Data Centre projects
4.	Experience of installation, configuration, Management and Monitoring of Windows/Linux based Servers with high availability solutions like clustering / load balancing of servers, Server Virtualization (using Hyper-V/VMware /Open Source)
5.	Experience of administration and management of Windows/Linux based Servers
6.	<p>Extensive Knowledge of IIS Web Server for successful running &amp; administering WWW, FTP, SMTP etc. services on production environment. Databases like MS SQL/MySQL/Maria DB/PostgreSQL/Oracle etc. connectivity for applications running on Web/App servers.</p> <p style="text-align: center;">Or</p> <p>Extensive Knowledge of Apache Web Server, Tomcat &amp; JBoss Application Server for successful running &amp; administering WWW, FTP, and SMTP etc. services on production environment. Databases like MySQL/Maria DB/PostgreSQL/Oracle etc. connectivity for applications running on Web/App servers.</p> <p style="text-align: center;">Or</p> <p>Extensive Knowledge of DAMP (Drupal + Apache + MySQL + PHP) setup, Operations &amp; Maintenance for Drupal related server administration covering administering WWW, FTP, SMTP etc. services on production environment.</p>

S. No.	Description
	Databases like MySQL/Maria DB/PostgreSQL/Oracle etc. connectivity for applications running on Web/App servers.

#### 12.1.4 Network Admin - L2

S. Np	Description
1.	B.E./B. Tech./MCA or higher degree from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications
3.	Minimum 6 years of IT experience out of which 3 years as Network Administrator in Government domain
4.	Must have sound knowledge of switching, routing, QoS, OSPF, BGP, NAT, Virtual Networks, Net Flow, etc.
5.	Must have minimum 3 years of hands on experience with L3 Switches
6.	Must have sound knowledge of system administration, shell scripting, python, ansible, puppet, Application load balancing, routing, IP tables, HTTP/HTTPS, SSL offloading, web-server, TCP multiplexing, etc.

#### 12.1.5 Security Specialist - L2

S. No.	Description
1.	B.E./B. Tech./MCA or higher degree from a recognized university
2.	Certified Security Professional with one of the certification, namely, a) ECSA b) CEH c) CISA d) CISSP e) OEM certification in security
3.	Minimum 5 years of IT experience out of which at least 3 years as a Security Administrator in Government sector
4.	Knowledge of operating systems, network devices and security devices
5.	Knowledge of Networking protocols
6.	Knowledge of troubleshooting and management of network technologies
7.	Knowledge of configuration, operations, troubleshooting and resolution of network security appliances such as firewall, IPS, DDoS, SIEM, Anti-Virus, Patch Management, Application firewall etc.

#### 12.1.6 DB Administrator - L2

S. No.	Description
1.	B.E./B. Tech./MCA or higher degree from a recognized university
2.	Certification in Database Administration
3.	Minimum 6 years of IT experience out of which 3 years as Database Administrator in Government sector

S. No.	Description
4.	Experience of installation, configuration, Management and Monitoring of Windows based Database software i.e. MS SQL Database Server with high availability solutions like clustering/Mirroring of servers. Creation & Management of database accounts, Backups/log-shipping. Or Experience of installation & configuration of Linux based MySQL/PostgreSQL/Oracle Database/application Server software with high availability solutions like Clustering/load balancing/log-shipping of servers
5.	Extensive Knowledge of administration and management of Windows /Linux based Database Servers. Knowledge of related/dependent OS services.
6.	Knowledge of IIS/Apache/Tomcat Web Server for http services etc. for integration with Web/Application Server

#### 12.1.7 Video Analyst / IP camera Surveillance Expert - L3

S. No.	Description
1.	B.E./B. Tech./MCA or higher degree from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications
3.	Minimum 6 years of IT experience out of which 3 years in IP camera / Video surveillance
4.	Must have sound knowledge of Video Analytics, IP Camera Surveillance, video storage & archiving, command/control display technologies and general Security system principles and practices
5.	Must have minimum 3 years of hands on experience in IP camera Surveillance/ Video Analytics , ability to customize analytics on cameras and integrate with third party systems
6.	Must have sound knowledge of WAN, LAN, firewall, network switch technologies and video transmission on IP networks etc.

#### 12.1.8 Software Developer (Full Stack Developer) - L3

S. No.	Description
1.	B.E. or B. Tech. with MBA or equivalent / M.E. or M.Tech / MCA or higher degree from a recognised university
2.	Should have experience of working the IT infrastructure / Data Centre / Smart City Solutions / Surveillance
3.	Industry accredited certifications like MCSD , Oracle Certified Expert/Professional
4.	Minimum 8 years' experience as a Full Stack Developer with experience in middleware , database integration and front-end development
5.	Should have minimum of two years of experience within the organization

S. No.	Description
6.	Should have minimum 2 years' experience on projects related to ICCC command control software used by MSI
7.	Should not serve in any other capacity under this Contract
8.	Should have more than 3 years of experience in middleware integration projects and API based integration

#### 12.1.9 Support Engineer – L1

S. No.	Description
1.	B.E./B. Tech./MCA or Diploma in computer science, electrical or electronic or information technology or computer technology from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications
3.	Minimum 3 years of experience out of which 2 years in L1 computer hardware and software support/LAN/servers/storage/video walls surveillance/IT help desk support/Video conference
4.	Must have knowledge of Video walls, PC's, LAN, servers, storage, IP telephony, help desk,

#### 12.1.10 Electrical Maintenance Engineer

S. No.	Description
1.	Any Diploma from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications
3.	Minimum 6 years of experience in maintenance electrical substation, distribution, UPS, DG, other BMS systems
4.	Must have knowledge of basic computer word, excel, BMS software and help desk
5.	Should have a lead a team size of 3 members, at least one project
6.	Should have basic knowledge about frisking, emergency situation response, records book keeping
7.	Should be able to coordinate with different vendors

#### 12.1.11 HVAC Technician

S. No.	Description
1.	Any Diploma from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications
3.	Minimum 6 years of experience in maintenance of HVAC and other BMS systems
4.	Must have knowledge of basic computer word, excel, BMS software and help desk

S. No.	Description
5.	Should have a lead a team size of 3 members, at least one project
6.	Should have basic knowledge about frisking, emergency situation response, records book keeping
7.	Should be able to coordinate with different vendors

#### 12.1.12 EMS Support Engineer – L2

S. No.	Description
1.	Any Engineer from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications in EMS Software and Hardware
3.	Minimum 3 years of experience in EMS solutions for data centre by managing and monitoring servers, database, network , security components and their SLA monitoring
4.	Must have knowledge of good knowledge of computer word, excel, EMS software, help desk and incident management. Shall be responsible for generating SLA reports on regular basis

#### 12.1.13 BMS Support Engineer – L2

S. No.	Description
1.	Any Engineer from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications in BMS Software and Hardware
3.	Minimum 3 years of experience in maintenance electrical distribution, UPS, DG, HVAC, IP camera, other BMS systems using software based integrated BMS monitoring solutions
4.	Must have knowledge of good knowledge of computer word, excel, BMS software , help desk and incident management

#### 12.1.14 Helpdesk Staff

S. No.	Description
1.	Any Diploma from a recognized university
2.	Respective OEM Certified Professional or equivalent certifications in Helpdesk Software functions
3.	Minimum 3 years of experience in IT Helpdesk functions , with proficiency in Hindi, English and Punjabi
4.	Must have knowledge of basic computer word, excel, Helpdesk software and Incident Management

**12.1.15 Security Staff**

S. No.	Description
1.	Any Diploma from a recognized university or 10 <sup>th</sup> standard Pass
2.	Should have completed security services related training for 1 month

### 13. Annexure VI: Location Details of Public Address System

S. No	Name of the Location	Quantity
1.	Hall bazaar	3
2.	Saragadi Parking (Below)	1
3.	Heritage walk	1
4.	Crystal chowk	1
5.	Queens road	2
6.	Giani Tea Stall	1
7.	Putligarh - kichloo chowk - Khandwala chowk (20 mtrs - 30 mtrs)	1
9.	Durgiana mandir	1
10.	Lohgarh chowk	1
11.	Bus stand (In gate, out gate, Center)	3
12.	Railway station (In gate, out gate, Parking)	3
13.	Link road	1
14.	Malls - Celebration, Alpha, Trillium	3
15.	Majitha road (Makkan restaurant)	1
16.	Gurudwara Shaidwara sahid	1
17.	Islamabad flyover	1

## 14. Annexure VII: Location Details of Public Address System

- I. All the network cameras supplied must be certified for: FCC , CE and UL ( Certificates to be enclosed)
- II. The network cameras for 720P HD and 1080P HD supplied must meet the SMTPE video standards: SMTPE 296M (HDTV 720p) & SMTP 274M HDTV 1080P).
- III. The network cameras supplied must meet either of below conditions on compression standards:
  - ISO/IEC 23008-2, ITU-T H.265 or
  - ISO/IEC 14496-10 AVC (H.264) video compression standards with suitable optimization to achieve 3 Mbps or lower bit rate at 1920X1020 resolution at 30 FPS.
- IV. The network cameras supplied must meet the IEC 60529 (IP66) environmental protection standards.
- V. The network cameras supplied must be manufactured in accordance with the ISO 9001&14000 standards.
- VI. The network cameras supplied must be compliant with 2002/95/RoHS.
- VII. The Camera Shall Support 3rd Party Edge Analytics
- VIII. The cameras shall support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.
- IX. The unit shall provide centralized certificate management, with both pre-installed CA certificates and the ability to upload additional CA certificates. The certificates shall be signed by an organization providing digital trust services.
- X. The Camera shall support IEEE 802.1X authentication, Password protection, IP address filtering, HTTPS encryption, Digest authentication, User access log, Centralized certificate management
- XI. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
- XII. The implemented API shall be standardized and supported by all network video products offered by the manufacturer
- XIII. The PTZ network surveillance cameras must have minimum RAM on processor 512 MB RAM, 128 MB Flash or better for better performance of the camera.
- XIV. The network surveillance cameras must support minimum On Board Edge storage of 128 GB or better.
- XV. The specified unit shall be of manufacturer's official product line, designed for commercial and/or industrial 24/7/365 use.
- XVI. The specified unit shall be based upon standard components and proven technology using open and published protocols and adopt to industry established standards.
- XVII. All cameras must comply with ONVIF Profile S standard or better.
- XVIII. Firmware/software upgrades are to be provided by the OEM free of cost during the warranty period and AMC Period. Undertaking from OEMs to be provided on their Letter head

- XIX. All the major components of the CCTV systems shall be latest but field-proven and shall not be End-of-Life / Outdated; the same shall have to be supported by concerned OEM for at-least 5 years' period from the date of supply.
- XX. All the cameras shall have 5 Years OEM warranty and the same shall be submitted on OEM Letter head.
- XXI. Cameras shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.
- XXII. Camera OEM to be present in India for at least 7 years and a subsidiary of the parent company and not through Joint venture or Distributor. Camera OEM should submit a declaration letter along with letter of incorporation confirming the same.
- XXIII. OEM of CCTV shall provide RMA Support response in 4 Working days with Advance Replacement Policy and shall provide duly certified document by OEM/Manufacturer.
- XXIV. All the cameras shall have ability to change the GOP/ GOV for Bit rate optimization.
- XXV. All Fixed cameras shall have ability to select user defined shape for motion detection to include or exclude area to reduce false alarms, bandwidth and storage.
- XXVI. All cameras shall have ability to send and receive triggers to perform any action without intervention of VMS.
- XXVII. Vendor should submit technical compliance on OEM letterhead for all major items i.e. Camera, VMS, Switch, Wireless, Storage and passive items.
- XXVIII. Bidder Should Submit Valid authorization in original form from all major Items i.e. Camera, VMS, Switch, Wireless, Storage and passive items
- XXIX. Minimum 3 streams required from the camera.
- XXX. Camera OEM to have at least 15 employees in India and a local RMA centre. OEM's Service tax registration document clearly mentioning service tax no. to be given as proof.
- XXXI. MAC address of the cameras should be in the name of the CCTV OEM company supplying the cameras. Declaration to be submitted along with MAF. To be cross-verified at the time of POC.
- XXXII. Bidder along with OEMs of major items (like IP Camera of all types, VMS, Video Analytics, Servers, Storages, switches etc.) should not be blacklisted by any Ministry under Government of India or by Government of any State in India or any of the Government PSUs as on tender floating date. Certificate / affidavit mentioning that the Bidder is not blacklisted by any Ministry under Government of India or by Government of any State in India or any of the Government PSUs.
- XXXIII. OEM of IP camera must be ISO 9001:2008 certified. Documentary proof to be submitted.

## 15. Annexure VIII: Indicative ICCC Room Layout

