PROJECT MANAGEMENT CONSULTANT (PMC) FOR ASSISTING LUDHIANA SMART CITY LIMITED (LSCL) TO DESIGN, DEVELOP, MANAGE AND IMPLEMENT SMART CITY PROJECTS UNDER SMART CITY MISSION (SCM) IN LUDHIANA CITY OF PUNJAB

Detailed Project Report (DPR)

for

Integrated Command & Control Centre With SMART Components

Version – 12

November 2018

Submitted by

AECOM Asia Company Limited

In JV with

AECOM India Private Limited
&
PricewaterhouseCoopers Private Limited

Table of Contents

Quality information

Prepared by	Checked by	Approved by
Sushil Khachane	Vijay Sharma	Sanjay Verma

Revision History

Version	Date	Name	Company	Role	Summary of Changes
V1	16/12/2016	Atul Gupta	PwC	IT Expert & SME	Initial draft
V2	30/12/2016	Atul Gupta	PwC	IT Expert and SME	LED Street Light Project Removed from ICCC Project
V3	25/03/2017	Atul Gupta	PwC	IT Expert and SME	Revised Costing as per PMIDC Inputs
V4	26/04/2017	Atul Gupta	PwC	IT Expert and SME	Revised DPR incorporating Changes suggested by SEMT team
V5	08/05/2017	Atul Gupta & Vaishalik Jain	PwC	IT Expert and SME	Revised Cost Model basis discussion with Mr. Shyam MoUD
V6	21/07/2017	Gaurav Singhal	PwC	IT Expert and SME	O&M of Safe City Project Included in the Scope as per directives from PMIDC on the meeting held on 02/06/2017
V7	16/03/2018	Gaurav Singhal	PwC	IT Expert and SME	SMART Components included as part of Project post discussion with CEO PMIDC on 05/02/2018
V8	23/04/2018	Gaurav Singhal	PwC	IT Expert and SME	Revised Project Cost as per inputs from CEO PMIDC and Excluded Safe City O&M as per Meeting held on 23/03/2018 in PMIDC Chandigarh
V9	06/05/2018	Gaurav Singhal	PwC	IT Expert and SME	Changes as per feedback from ADC Ludhiana (MOM Attached as part of DPR)
V10	14/06/2018	Gaurav Singhal	PwC	IT Expert and SME	Revised Project cost and specifications as per the Meeting held on 09/06/2018 in PMIDC Chandigarh
V11	18/06/2018	Gaurav Singhal	PwC	IT Expert and SME	Revised project cost and specifications as per the Industry workshop held on 15/06/2018 at PMIDC Chandigarh
V12	13/11/2018	Sushil Khachane	AECOM	IT Expert and SME	Revised project cost and specification as per discussion held with Advisor (Tech) to Hon. Chief Minister, Punjab, PMIDC & DoGR on 29/10/2018, 30/10/2018, 05/11/2018 & 06/11/2018 at PMIDC Chandigarh

Review History

Version	Date	Name	Role	Company
V1	28/03/2017	Suketu Modi	Associate Director	PwC
V6	20/07/2017	Suketu Modi	Associate Director	PwC
V8	26/04/2018	Rajinder Banyal	Associate Director	PwC
V9	07/05/2018	Rajinder Banyal	Associate Director	PwC
V10	14/06/2018	Rajinder Banyal	Associate Director	PwC
V11	18/06/2018	Rajinder Banyal	Associate Director	PwC
C12	14/11/2018	Vijay Sharma	Associate Director	AECOM

Approval History

Version	Date	Name	Role	Company
V12	14/11/2018	Sanjay Verma	Team Leader	AECOM

Distribution List

# Hard Copies	PDF Required	Association / Company Name
1	Yes	Chief Executive Officer Ludhiana Smart City Limited, Ludhiana, Punjab

This document has been prepared solely for Ludhiana Smart City Limited (LSCL), being the express addressee to this document. AECOM does not accept or assume any liability, responsibility or duty of care for any use of or reliance on this document by anyone, other than (i) LSCL, to the extent agreed in the relevant contract for the matter to which this document relates (if any), or (ii) as expressly agreed by AECOM in writing in advance.

This publication (and any extract from it) may not be copied, paraphrased, reproduced, or distributed in any manner or form, whether by photocopying, electronically, by internet, within another document or otherwise, without the prior written permission of AECOM. Further, any quotation, citation, or attribution of this publication, or any extract from it, is strictly prohibited without AECOM's prior written permission.

AECOM

Acronyms & Abbreviations

Sl. No.	Particulars	Description
1	LSCL	Ludhiana Smart City Limited
2	PMC	Project Management Consultant
3	LMC	Ludhiana Municipal Corporation
4	ANPR	Automatic Number Plate Recognition
5	ATCS	Adaptive Traffic Control System
6	BOM	Bill of Material
7	CCTV	Closed Circuit Television
8	CCC	Command and Control Center
9	CONOPS	Concept of Operations
10	DC	Data Center
11	DRC	Disaster Recovery Center
12	FMS	Facility Management Services
13	GIS	Geographical Information Systems
14	GPS	Global Positioning System
15	GSM	Global System for Mobile Communication
16	ICCC	Integrated Command and Control Center
17	ICT	Information and Communication Technology
18	IP	Internet Protocol
19	IT	Information Technology
20	ITMS	Intelligent Traffic Management System
21	KPI	Key Performance Indicator
22	MLCP	Multi-Level Car Park
23	MPLS	Multi-Protocol Label Switching
24	MSI	Master Systems Integrator
25	ONVIF	Open Network Video Interface Forum
26	O&M	Operations and Maintenance
27	OEM	Original Equipment Manufacture
28	OFC	Optical Fiber Cable
29	OWASP	Open Web Application Security Project
30	PKI	Public Key Infrastructure
31	PIS	Public Information System
32	PA System	Public Address System
33	PoP	Point of Presence

Sl. No.	Particulars	Description
34	PTZ	Pan Tilt Zoom
35	RFP	Request for Proposal
36	RLVD	Red Light Violation Detection
37	RTO	Recovery Time Objective
38	RPO	Recovery Point Objective
39	SCADA	Supervisory control and data acquisition
40	SLA	Service Level Agreement
41	SMS	Short Message Service
42	SOP	Standard Operating Procedures
43	TPA	Third Party Auditor
44	UAT	User Acceptance Testing
45	UPS	Uninterrupted Power Supply
46	VM	Virtual Machine
47	VMD	Variable Message Display
48	VCA	Video Content Analysis

1. Introduction

1.1 Project Background

The city of Ludhiana has emerged as Punjab's core city as an important center of trade and commerce in Northern India. Ludhiana city which is district headquarters is the hub of industry in Punjab. Ludhiana is the biggest city of the State, It has eight tehsils, seven sub-tehsils and twelve development blocks. Ludhiana has been selected among the top 20 smart cities in India for which it receives funding from Ministry of Housing & Urban Affairs (MoHUA), Government of India for projects under its smart city proposal. Ludhiana smart city proposal includes several Pan City and Area Based Development initiatives with a focus on both infrastructure and ICT advancements in the city and at strategic locations. Most of the ICT initiatives proposed and being implemented by Ludhiana city have been identified with a predominant objective to improve public safety and surveillance, traffic management, public services quality, emergency response and real time tracking of services.

In order to meet the deficiencies of the present system, namely, lack of integrated systems, inefficient work procedures, lack of up-to-date and accurate databases, lack of data sharing, etc., ICT initiatives such as the Integrated Command and Control Centre along with smart features with specific focus on real time tracking of services, smart lighting, and many more have been proposed by the city. This document covers detail scope, specifications of the proposed for ICT initiatives of Integrated Command and Control Center (ICCC) and Project Management Strategy.

1.2 Project Objectives

The key objective of this project is to establish a collaborative framework where input from different functional departments such as transport, water, fire, police, e-governance, etc. can be assimilated and analysed on a single platform; consequently resulting in aggregated city level information. Further this aggregate city level information can be converted to actionable intelligence, which would be propagated to relevant stakeholders and citizens. Following are the intangibles that should be addressed by this intervention:

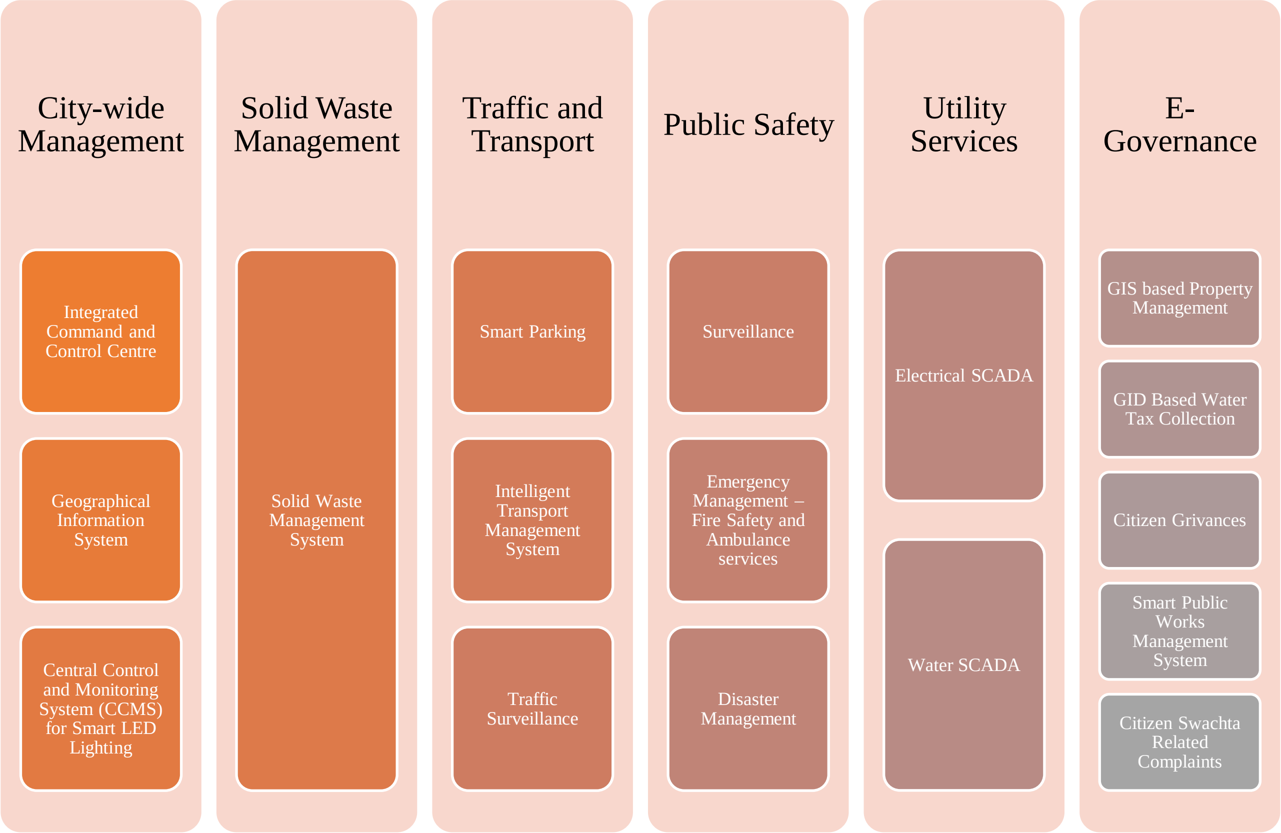
- Better management of utilities and quantification of services
- Disaster Management and Emergency Response System
- Efficient traffic management
- Enhanced safety and security
- Real Time Asset Management
- Integration with existing control centres and other systems in the city (with provision for future scalability)
    - Smart Lighting,
    - Smart Governance,
    - City Surveillance and smart traffic (RLVD and ANPR),
    - Solid Waste Management,
    - Smart Parking,
    - City Bus ITMS,

- ○ Water SCADA
- ○ Sewerage,
- ○ Power SCADA
- ○ Health,
- ○ Education
- ○ GIS
- ○ Unified operations through integration of urban functions offered by the city administration

Ludhiana SMART City Project envisages deployment of following components to achieve the objectives:

- Deployment of various sensors (environment and weather sensors) throughout the city to improve situational awareness
- Deployment of Public Addressal System & Panic Button with Emergency Call Box to enhance public awareness and emergency response.
- Deployment of Various Cameras in municipal limits to improve various civic services like Solid Waste Management, Tahbazari Violations, etc.
- Deployment of Variable Messages Signboards for Public Information Display.

Following city-wide domains will be covered under the scope of this project through ICT interventions. There may be other building blocks which are not presented in the below diagram.



City-wide Management

- Integrated Command and Control Centre
- Geographical Information System
- Central Control and Monitoring System (CCMS) for Smart LED Lighting

Solid Waste Management

- Solid Waste Management System

Traffic and Transport

- Smart Parking
- Intelligent Transport Management System
- Traffic Surveillance

Public Safety

- Surveillance
- Emergency Management – Fire Safety and Ambulance services
- Disaster Management

Utility Services

- Electrical SCADA
- Water SCADA

E-Governance

- GIS based Property Management
- GID Based Water Tax Collection
- Citizen Grivances
- Smart Public Works Management System
- Citizen Swachta Related Complaints

1.3 Key Observations & Gaps identified

The traditional operating model for a city has been based around functionally-oriented service providers that operate as unconnected vertical silos, which are often not built around user needs. Integrated City Command and Control Centre propose to develop new operating models that drive innovation and collaboration across these vertical silos.

Traditionally, budget-setting, accountability, decision-making and service delivery have been embedded within vertically-integrated delivery chains inside cities – delivery silos which are built around functions not user needs. As illustrated in Figure –

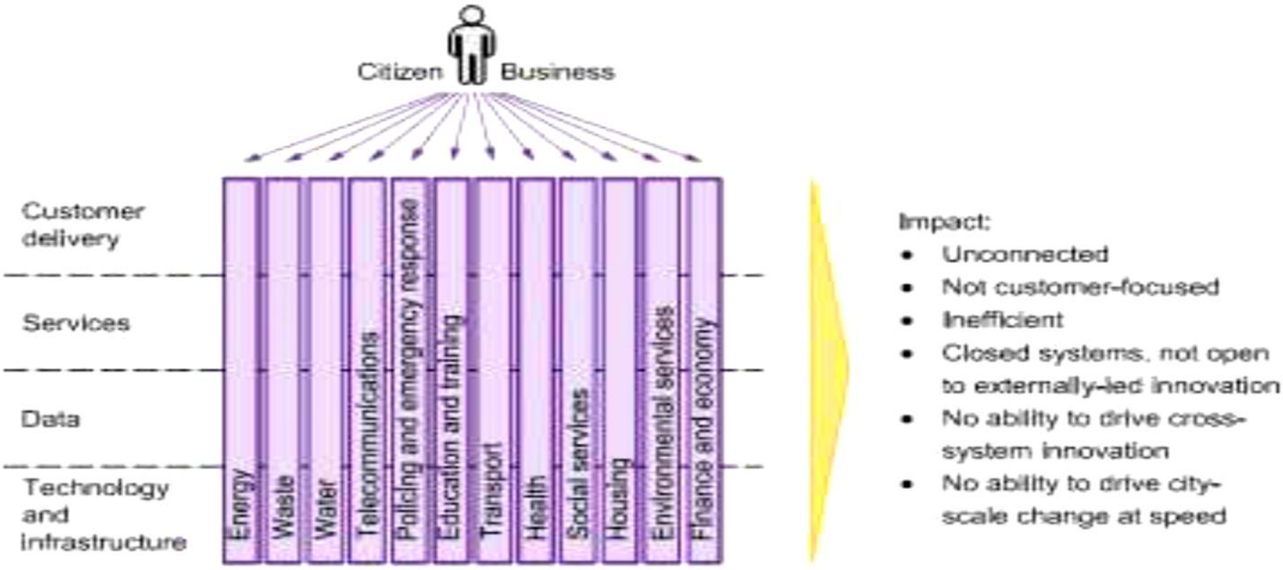


Figure 1: Traditional Operating Model

- The individual citizen or business has had to engage separately with each silo: making connections for themselves, rather than receiving seamless and connected service that meets their needs;
- Data and information has typically been locked within these silos, limiting the potential for collaboration and innovation across the city, and limiting the potential to drive city-wide change at speed.

The Existing Systems: Integration Opportunities

In this study, we investigated the scope of different aspects of integration.

Ludhiana has many existing – System and need to focus on added benefit from integration of system into a single system data sharing and operational "platform" – effectively the "Data Model" or "Data hub". This uses an open source approach that will provide the single window for any user of data but without large capacity outlay.

The existing system is yet to fully integrate all the data and output channel it could use. The opportunity to integrate multiple sub -systems like ITMS, Waste management, SCADA systems will take some time to go live.

Based on the understanding of the existing traditional system it is important to have an integrated City Command and Control system in place to provide the best in class services of Infrastructure to the citizen of Ludhiana.

The Need

The city needs to establish governance processes which enable technology and digital assets to managed city wide resources on a real time basis through the Integrated City Command and Control Centre. In order to setup ICCC city need to do an agile integration considering the following areas:

Ensure all the systems are working to their optimum in terms of use data from other systems and exporting information for wide use – in line with open data policies. A good example here is making the most of the strategy selection tool in the city traffic system, which can take input from variety of yet untapped source and system.

- Identify the important parameters of the system to add for integration with master systems
- Internal department to make their data digitized to be processed through the ERP or other relevant systems
- Enables integration with different systems such as Emergency response system, Municipal applications etc.
- Integrated Platform for real time city operations, collaborative decision supports and advanced simulation and optimization – real-time operations hub and enterprise knowledge hub
- Unified Big Data Platform for structured, semi-structured and unstructured data with high volume and velocity
- Real time Situational Awareness and pre-built extendable SOPs
- 2D / 3D locational intelligence and analytics with time series analysis for Smart City Operations planning and management
- Embedded Data Lake that brings single source of truth from heterogeneous systems – provides flexibility to leverage data by various departments / stakeholders for Operational Excellence
- Prebuilt KPI Manager with role-based configurable / customizable Smart City Operations dashboards

1.4 Benefits envisaged

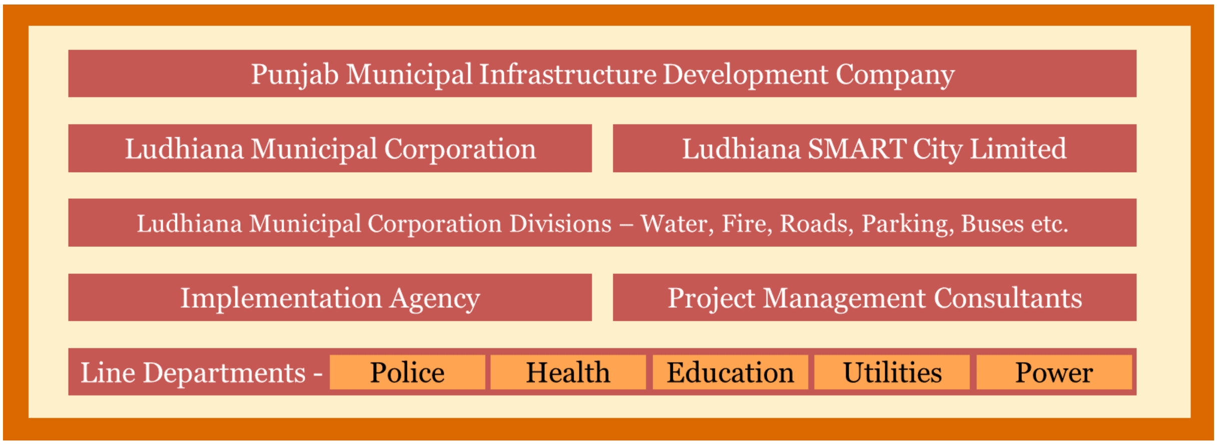
CCC enables collation of information and collaborative monitoring, thus helping in the analysis of data for quicker decision making. Intelligent operations capability ensures integrated data visualization, real-time collaboration and deep analytics that can help different stakeholders prepare for exigencies, coordinate and manage response efforts, and enhance the ongoing efficiency of city operations. The interface at ICCC gives a real-time and unified view of operations. Cities can rapidly share information across agency lines to accelerate problem response and improve project coordination. Furthermore, the ICCC will help in anticipating the challenges and minimizing the impact of disruptions.

Following are the benefits envisaged from ICCC:

- Enable real time monitoring of the various facets of management of Ludhiana Smart City i.e. Security, Traffic and City Utilities
- Provide capability to respond in a unified manner to situations on ground (both day to day and emergency situations) by creating a common operational picture for the relevant stakeholder
- Provide and manage touch points from all concerned stakeholders during the lifecycle of various incidents
- Define and manage the Key Performance Indicators (KPIs) for various operational aspects of the City Management
- Provide capability to conduct analysis for continuous improvement of city operations

1.5 Identification of all stakeholders

The project requires collaboration between multiple stakeholders for its successful execution. It is therefore important to understand the various stakeholders envisioned to be part of this project and the role that they are expected to play. Following are the critical stakeholders whose involvement will drive the project and enable the establishment of strong project governance:


Punjab Municipal Infrastructure Development Company

Ludhiana Municipal Corporation

Ludhiana SMART City Limited

Ludhiana Municipal Corporation Divisions – Water, Fire, Roads, Parking, Buses etc.

Implementation Agency

Project Management Consultants

Line Departments - Police Health Education Utilities Power

Ludhiana Municipal Corporation (LMC)

The Ludhiana Municipal Corporation will be responsible for the driving the project along with the Ludhiana SPV. LMC would also be responsible for driving maximum usage and adoption of the ICT functions across the city departments. LMC departments are critical for driving adoption and will be the end users of this project. The direct benefit of the project will be felt at each of the department. The project will be a support to the functioning of departments given below.

The reach and users of these projects will be at offices of various LMC departments

- ✓ Disaster Management
- ✓ Environment
- ✓ Fire
- ✓ Public Transport (Buses)
- ✓ Roads
- ✓ Sewerage
- ✓ Solid Waste Management
- ✓ Storm Water
- ✓ Traffic
- ✓ Water
- ✓ Assessment & Collections (Professional Tax, Shops & Establishment, Property Tax)
- ✓ Building Approvals
- ✓ Finance
- ✓ License Issuance
- ✓ Public Relations

Smart City SPV

As per the GoI guidelines, a separate Special Purpose Vehicle (SPV) has been created for execution of projects under the smart city mission for the city of Ludhiana. This SPV shall carry end to end responsibility for implementation, operationalization and utilization of the proposed project along with efforts and assistance of the PMC. PMC will support the SPV for executing the tendering process for the selection of the implementation partner. Thereafter, during the implementation phase and SPV be responsible for carrying out the review of detailed design, deployment, acceptance testing and providing support during the final acceptance tests. During the O&M phase, the SPV will engage the PMC with the responsibility to review the maintenance and operations and driving the adoption of the projects.

Implementation Agency

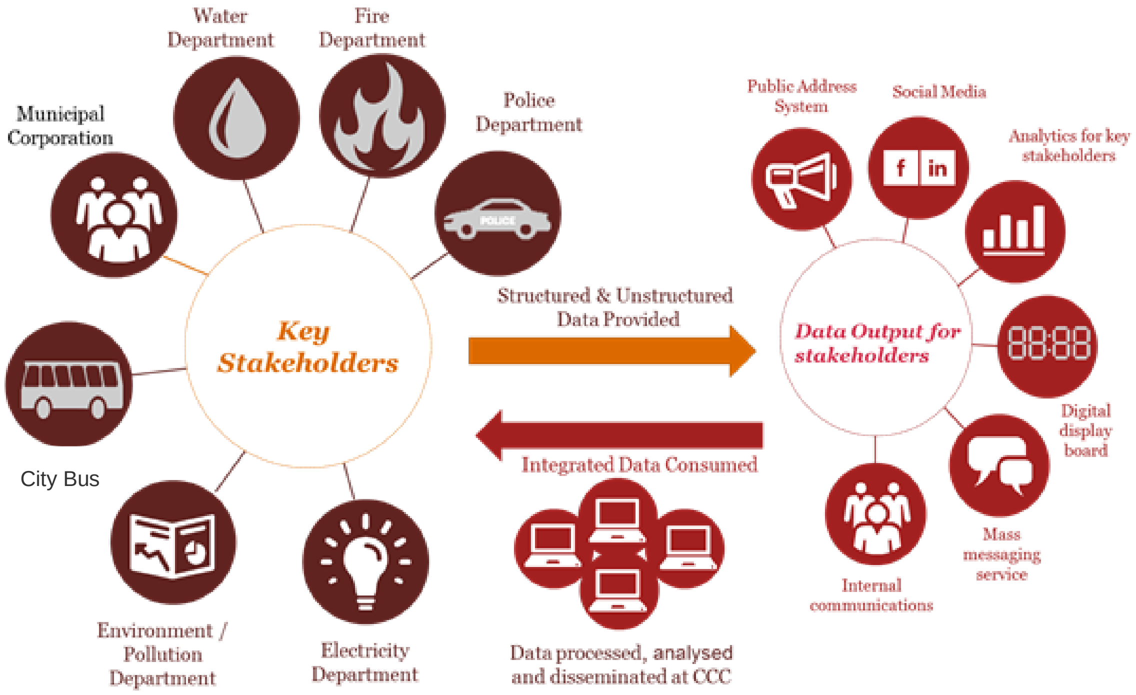
An implementation partner for the project shall be selected by the SPV through an open competitive bidding process. This may be a single agency or a consortium of multiple agencies that would come together for project execution on commercial terms.

The implementation partner would be the primary owner for detailed project design and the execution of the project on ground. It will be responsible for providing the necessary guidelines and support during the acceptance testing for integration of Core system to each of the sub systems. Thereafter, in the O&M phase of the project, the implementation partner will act as the primary owner for maintenance and operations.

Project Management Consultant

Project Management Consultant shall be responsible for overall Project Design, RFP Preparation & Bid process management and vendor on-boarding.

Key Stakeholders & Data flow



2. Scope

The scope of this DPR may be divided based on the stakeholders of the project and scope of work:

Stakeholders: The primary stakeholders of this projects are Punjab Municipal Infrastructure Development Company (PMIDC), Govt. of Punjab, Ludhiana Smart City Limited (LSCL) , Ludhiana Municipal Corporation (LMC) and citizens of Ludhiana City. Following table describes the primary stakeholders and their interest level/roles.

Sl. No.	Primary Stakeholder	Interest/ Role
1	Citizens	Quality/ value/ time taken to receive services, provision for customer care, Improved city services
2	PMIDC, Govt. of Punjab LSCL LMC LMC Departments Employees of above entities Other Departments	• Quality of service provided • Improved co-ordination with other departments, • Seamless connectivity with other IT projects/ Initiatives • Ease of providing services

Sl. No.	Primary Stakeholder	Interest/ Role
	Other Department Employees	• Reducing response time to provide services • Proactive actions for complaint resolution

The implementation strategy for ICCC is developed based upon the below quadrants under which various stakeholder groups fall as illustrated below:

High Interest-Low Influence	High Interest-High Influence
Citizen , PMC, MSI	LSCL, LMC ,PMIDC Officials
Low Interest-Low Influence	**Low Interest- High Influence**
Other Department Employees	Other Civic Representatives – Mayor, DC, CP

Roles & Responsibilities of key Stakeholders

Roles & Responsibilities of key Stakeholders

Stage	Roles and Responsibilities of Key Stakeholders			
	Master System Integrator	LSCL	Other Departments	PMC
Planning	• Define Project Implementation Plan • Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc. • Benchmark the city's current services against the Liveability Indicators identified in Annexure IX – Project Mapping to Liveability Standards in Cities • Develop the Concept of Operations (CONOPS) for the proposed Integrated Command and Control Centre • Providing physical layout of the ICCC (with 3D simulation) • Assessment of IT Infrastructure and Non IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement all locations (including buildings). • Formulation of solution architecture, detailed design of smart city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP	• Provide necessary information to MSI for doing surveys • Facilitate Interaction with other Departments for getting the required integration • Help MSI get necessary approvals for implementing ICCC. • Help MSI finalize the protocols for data exchange between ICCC and various other systems. • Review the documents submitted by MSI and provide feedback	• Provide necessary information to MSI for doing future integrations. • Provide necessary information to MSI for finalizing the data exchange between the systems.	• Prepare contract agreements • Prepare all relevant documents

Stage	Roles and Responsibilities of Key Stakeholders			
	Master System Integrator	LSCL	Other Departments	PMC
	documentation • MSI will define the formats for data exchange between various services and systems in agreement with LSCL.			
Implementation	• Adhere to defined SLAs and timelines • Physical Setup of ICCC as per the layout agreed with LSCL. • Helpdesk setup, procurement of equipment, edge devices, COTS software (if any), licenses. • Physical Security and Housekeeping setup • IT and Non IT Infrastructure installation, development, testing and production environment setup • Safety and security of IT and Non IT Infrastructure • Establishment and configuration of Network Connectivity (provided by service provider) as per service level between ICCC and various other applications for integration. • Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any) • User Manuals , training curriculum and training materials	• Provide building structure for setting up ICCC (based on agreed plan) • Provide necessary Electricity and Water Connection to the ICCC facility. • Provide necessary network connectivity as per the desired requirements between ICCC and other systems for integration • Facilitate Interactions with other Departments for getting the required integration. • Help MSI get necessary approvals for implementing ICCC. • Review the documents submitted by MSI and provide feedback. • Provide manpower for getting trained on ICCC operations	• Provide necessary access to the current ICT setup for integration with ICCC.	• Co-ordinate with Line department and MSI • Project Mgmt. • Review reports submitted by MSI • Submit status report to LSCL

Stage	Roles and Responsibilities of Key Stakeholders			
	Master System Integrator	LSCL	Other Departments	PMC
	• Role based training(s) • SoP implementation, Integration with GIS Platform, Integration of solutions with Command and Control Centre , KPI Development. • Facilitating UAT and conducting the pre-launch security audit of applications. • User training and roll-out of solution • Integration of the various services & solution with ICCC platform • Develop provisions for a scalable system			
Post – Implementation	• Deploying manpower • Security of ICCC premises • Annual technical support • Preventive, repair maintenance and replacement of hardware and software components • Provide a centralized Helpdesk and Incident Management Support till the end of contractual period • Recurring refresher trainings for the users and Change Management activities • Provide required access and information for Audits • Preventive, repair maintenance and replacement of non ICT components • Overall maintenance of the ICCC facility and continuity of operations as per SLAs.	• Facilitate Interactions with other Departments for getting the required integration. • Help MSI get necessary feeds for ICCC. • Help MSI get necessary approvals (if any). • Review the documents submitted by MSI and provide feedback • In case of any incident or disaster facilitate communication from ICCC to field agents (in case of absence of ICT setup with field agents) • Payment of utilities bills during the operations period	• Provide and receive (if applicable) data feeds to/ from ICCC to their current ICT setup in the predefined formats. • Perform needful action in case of any incident or disaster	Helping LSCL in technical knowledge transfer

Stage	Roles and Responsibilities of Key Stakeholders			
	Master System Integrator	LSCL	Other Departments	PMC
	• Monitoring of Network Connectivity (provided by service provider) as per service level and report the non-compliance. • Submit Quarterly Reports • Adhere to defined SLAs	(like electricity, telephone, internet, water, etc.)		

2.1 Scope of the Project

The scope of the project includes implementation of identified smart ICT solutions including establishment of city ICCC and integrate the implemented solutions with ICCC. Scope also includes conduct a detailed assessment of current state of city services being provided and accordingly plan, design a comprehensive technical architecture of ICCC so that relevant current and future ICT project may be integrated with ICCC. For various ICT solutions to be implemented, the MSI has to provide edge devices, network connectivity (Sensor to Data Centre) and application software and other required components. Compute and storage components of the solution shall be provided by MSI only. From ICCC to Ludhiana Police Command & Control Center connectivity will be provided by MSI, Internet connectivity at City ICCC would also be in MSI Scope.

As part of scope the MSI is expected to integrate various ICT initiatives of the city with ICCC. These ICT initiatives may be from other departments' services like Water, Electricity, Police, and Transport etc.

The MSI shall have the overall responsibility to design, build, implement, operate, and maintain the project (at city level) for a period of four years from the date of successful commissioning.

Following table provides the scope, objective and the high level scope for implementation of City Integrated Command and Control Centre:

Feature	Objective	High Level Scope
City Integrated Command and Control Center (City ICCC)	Key Objectives of the City ICCC: • To serve as a centralized decision making center which supports and strengthens coordination in response to incidents/emergency situations • To serve as central information, communication, incident management hub for LSCL • To provide integration points for other existing or proposed command center from other government agencies e.g. Police, Disaster, etc. • To serve as the centralized monitoring & decision making hub for managing equipment, devices, resources and assets • City ICCC will enable city administration and its stakeholders in the following: • Effective decision making • Delivering effective governance by aggregating various data feeds from	Setting up city ICCC with 16 operators control room and operations and maintenance of the command center for contract duration.

Feature	Objective	High Level Scope
	sensors and systems • Providing interface/ dashboards to generate alert & notifications in real time • Quick and effective response to emergency or disaster situation	

2.2 Integration with existing CCTV surveillance System

Ludhiana city have already CCTV surveillance system in place for the safety and security of the citizen. This system has been managed by the Ludhiana police department separately. It is important to have integration in place between existing control room and future ready ICCC. There are 5000 camera were envisaged out of which 1442 camera are already installed and managed by the police department and it is important to have dedicated connectivity between ICCC .

2.3 Project Phases

The project is envisaged to be completed in total 12 months and overall duration is divided into three phases- Phase- I (6 Months) ,Phase- II (3 Months) and Phase –III (3 Months)

S. No.	System Description	Phases
1.	Integrated Command and Control Center	Phase I
2.	GIS	Phase I
3.	Deployment & Integration of Field Level Edge Equipment (Cameras, PA System, Panic Button & Emergency Call Box, Environmental Sensors, and Digital Variable messaging Sign boards)	Phase I
4.	Integration with City Surveillance	Phase I
5.	Integration with SMART governance	Phase I
6.	Integration with SMART LED lighting	Phase I
7.	Integration with Smart Traffic	Phase I
8.	Integration with Solid Waste Management	Phase I
9.	Integration with Power SCADA	Phase II
10.	Integration with Water SCADA	Phase II

S. No.	System Description	Phases
11.	Integration with ITMS	Phase II
12.	Integration with SMART Parking	Phase III
13.	Integration with Smart HealthCare	Phase III
14.	Integration with Smart Education	Phase III

The overall project Implementation may be divided into following parts:

Planning Stage:

This stage includes study of assessment of current state of city services being provided, preparation of DPR and bid process management for selection of Master System Integrator for design and development of ICCC. Project Inception Report, Project Charter, Project concept understanding will be the first few documents at planning stage.

Requirement Gathering Stage

Detailed assessment of the business requirements and IT Solution requirements for the ICCC will be finalized during this stage. After this, functional requirements will be converted into technical requirements in the form of System Requirement Specifications (SRS) in consultation with LSCL and its representatives.

Development Stage

During development phase various prevailing Smart City individual solutions will be studied and the projects which are envisaged in near future under the Smart City Programme of Ludhiana city will be designed.

Integration and Testing Stage

The ICCC Application or City Operation Platform should be integrated with data feeds of the following Smart City systems envisaged under the Smart City Programme of Ludhiana smart city. City operation platform along with compute and storage capabilities shall be provided by the MSI. Integration of ICT solutions will be the responsibility of MSI.

Broadly there are three kinds of data feed possible from all of the above systems. The software solution provided by MSI should have the capability to integrate these all three types of data.

Video Feed	CCTV Cameras or other Cameras
Sensor Data	SWM Vehicles- GPS Sensors, RFID Data Smart Lights Sensor Data, Smart Parking Sensor Data etc.
Structured Data Packets	SCADA GIS Data, SWM (GPS Co-ordinates of vehicles), Alert messages, ITMS, E-Governance Module

Integration of Future IT initiatives

The software solution should be scalable and modular in structure and should be able to integrate other future IT initiative of Ludhiana Smart City.

Approach for Integrations

- For successful integration it is required to have protocol and component level compatibility between existing systems/control centres and the envisaged command and control centre in order to have one uninterrupted operating picture of the city at ICCC.
- The solution implemented will be scalable across all future integrations and demands that arise for technology solutions of LSCL that will augment to the city wide network of sensors.
- City services such as surveillance, parking sensors, variable sign boards ITMS and any future ICT initiatives which will act either as upstream or downstream interfaces to the Integrated Operations Platform will have compatible APIs to integrate with ICCC.

Integration Scope

Following is the service wise brief scope of integration for various initiative of Ludhiana Smart City:

Sl. No	List of Services	Brief of Scope for Integration
1	Integration of Smart Parking	• City ICCC will be required to integrate the Smart Parking solution. LSCL will provide the data, information necessary for integration. Integration will be the responsibility of solution provider (City Vendor) • ICCC application /City operation platform will be required to receive feeds on the status of parking across the city (feeds received from all the edge devices of the Parking Solution). • These feeds will provide information of available, non-available parking slots, functional and non - functional parking slots. • City ICCC will also be required get video feeds from the parking areas on real-time basis. It will be the responsibility of MSI to integrate video management software with city operation platform to have situational awareness of the city at all times. • These video feeds will also help monitor assets of LMC, and LSCL • All the information received will also be required to be mapped on the GIS map. • All the information received from the smart parking sensors will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC application or city operation platform should also be able to trigger the commands / alerts (if required)

Sl. No	List of Services	Brief of Scope for Integration
2	Integration of Smart Lighting	• ICCC will be required to integrate with Central Monitoring and Control System (CCMS) to receive multiple kinds of feeds from the LED street lights that will be deployed across the city • ICCC will be required to get information on the status of working of the installed LED lights, as well as other sensors. • All the information received will also be required to be mapped on the GIS map. • All the information received will also go into the Analytical layer which will help city in better planning and running of operations. • This initiative is managed by LSCL. • LSCL will provide the data, information necessary for integration. Integration will be the responsibility of MSI
3	Integration of Solid Waste Management Services	• ICCC will be required to receive feeds from sensors deployed at field like SMART bins and other GPS sensors on vehicles. • ICCC will also get other information which is received in the control room like fuel utilization of Vehicles. • All the information received will also be required to be mapped on the GIS map. • All the information received will also go into the Analytical layer which will help city in better planning and running of operations. Integration with city operation center will be the joint responsibility of solution provider (City Vendor) and city operation platform provider MSI.
4	Integration of City Solid Waste Management	• Cameras will be deployed for SWM monitoring at key locations across the city to monitor waste disposal. This has to be integrated with the ICCC facility.
5	Integration with Intelligent Transport Management System	• ICCC will be required to integrate to get City bus location feeds from Transport Management System (GPS based). • These feeds will be sensor based feeds on location of public transport vehicles, bus station information operations, etc. • All the information received from the command center will also go into the Analytical layer which will help city in better planning and running of operations. • ICCC / city operation platform should also be able to trigger the commands / alerts (if required) to the respective command center.
6	Integration with CCTV Surveillance (Police Dep't.)	• ICCC will also get real-time video feed from the control center of City Surveillance (Police Dept.) • These video feeds will not be saved, but will be utilized in Analytical layer to help administration monitor its assets and do a better urban planning. • City ICCC will also be required to send video feeds received

Sl. No	List of Services	Brief of Scope for Integration
		from Smart Parking, SWM, City Surveillance in real-time basis to the command center of Traffic (if required). • These video feeds will also help monitor assets of LMC, and LSCL • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • ICCC will be required to integrate with Command Center of CCTV System (Police Department), to receive real-time feeds of the camera installed by them.
7	Integration with Emergency Response and Disaster Mgmt.	• ICCC will be required to integrate with Vehicle Tracking System of the Emergency Response and Disaster Management to send them alerts and notifications for any emergency / incidents / disaster in the city for doing required action. • ICCC system should also be able to get acknowledgement from the receivers. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • Integration of City Operation platform/ICCC with Emergency Response and Disaster Management will be the responsibility of MSI.
8	Integration with SCADA Systems	• ICCC will be required to integrate Water /Power (SCADA) control room to get all kinds of sensor feeds. • ICCC should be able to map this information on the GIS layer and help authority monitor the water /Power management of the city. • ICCC should also be able to trigger the commands / alerts (if required) to the respective command center. • All the information received from the application will also go into the Analytical layer which will help city in better planning and running of operations. • Integration of City Operation platform/ICCC with Emergency Response and Disaster Management will be the responsibility of MSI.

3. Proposed Solution

Smart ICT Solutions

The LSCL has identified certain Smart ICT intervention required to make the city smart. Functional and technical requirements have been identified. ICCC will be developed for Ludhiana smart city comprising of various Components packaged under 3 levels of interventions:

3.1 Level 1: Integrate and View

Certain components will be integrated using direct feeds, dashboards and sharing of alerts/ actionable inputs for integrate and view operations, such as:

1. City Surveillance System (Police and Traffic)
2. Smart Governance (E-Governance)
3. Intelligent Transport Management System – City buses
4. Smart Energy (Power SCADA)
5. Smart Water (Water SCADA)
6. SMART Health
7. SMART Education

3.2 Level 2: Integrate Command and Control

8. SMART Parking & Payment System
9. CCMS for LED Street Lights
10. GIS Based Property Management System
11. Smart Solid Waste Management – GPS Enabled Vehicle

3.3 Level 3: Implement, Command, Control and Fully Operate

12. Integrated Command and Control Center (ICCC)
13. Geographical Information System (GIS) Panic Button & Emergency Call Box
14. Public Addressal Systems
15. Environmental Sensors
16. Digital VMD's
17. CCTV Cameras Installed for various other civic purposes as part of Project

4. Design Considerations

The key systems and components envisaged for the Integrated Command & Control (ICCC) project, including expected system users, are shown in the component architecture diagram below for illustration purposes. Please note that this functional architecture is indicative in nature and is given in this report to bring clarity on the overall scope of project and its intended use. The detailed Technical Architecture would be designed by the selected Master System Integrator (MSI) in consultation with LSCL and its consultants and following minimum design principles would be followed for designing the comprehensive ICCC system for Ludhiana Smart City.

1. Scalability:

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

The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of delivering high performance till the system is operational. In this context, it is required that the application and deployment architecture should provide for Scale-Up and Scale out on the Application and Web Servers, Database Servers and all other solution components. The data centre infrastructure shall be capable of serving the growing concurrent users requirement which would be increasing as the city would grow.

2. Availability:

The architecture components should be redundant and ensure that are no single point of failures in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The MSI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data center components level.

3. Security:

The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. MSI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. The virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. LSCL would carry out the security audit of the entire system upon handover and also at regular interval during O&M period. Bidder's solution shall adhere to the model framework of cyber security requirements set for Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development).

Field equipment installed through the ICCC project would become an important public asset. During the contract period of the Project the MSI shall be required to repair / replace any equipment if stolen / damaged/faulty. Appropriate insurance cover must be provided to all the equipment's supplied under this project.

The systems implemented for project should be highly secure, considering that it is intended to handle sensitive data relating to the city and residents of the city. The overarching security considerations are described below:

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

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

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

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

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

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

The recommended guidelines for Cyber Security requirements for Ludhiana Smart City ICCC project as provided in Annexure 2 of this document.

4. Manageability:

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

5. Interoperability:

The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements.

6. Universal Access IT Systems:

The solution designed should ensure Universal Access to IT systems to empower citizens of Ludhiana city with disability to access the various systems/components envisaged and future systems for integrations with ease.

7. Open Standards:

Systems should use open standards and protocols. Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The MSI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should at least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time)

8. Single-Sign On

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

9. Support for PKI-based Authentication and Authorization:

The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the MSI for officials/employees involved in processing citizen services.

10. Convergence:

LSCL has already initiated many projects which have infrastructure at field locations deployed under them. The ICCC Infrastructure should be made scalable for future convergence needs. Under the smart city program, LSCL has envisaged to create a state of the art infrastructure and services for the citizens of Ludhiana, hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Hence the MSI is required to ensure that such infrastructure will allow for accommodation of equipment's being procured under other smart city projects. Equipment like Junction Boxes and poles deployed under the ICCC project at the field locations will be utilized to accommodate field equipment's created under the other projects of LSCL. The procedure for utilization of the infrastructure will be mutually agreed between the LSCL and Master System Integrator.

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

   i. Passive networking & civil work during implementation and O&M period,

   ii. Viewing manpower at CCC/ICCC / viewing centers during post-implementation

   iii. FMS staff for non- IT support during post-implementation

   iv. Services of professional architect for design of CCC/ICCC/Viewing centers

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

11. GIS Integration:

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

12. SMS Gateway Integration

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

13. Application Architecture

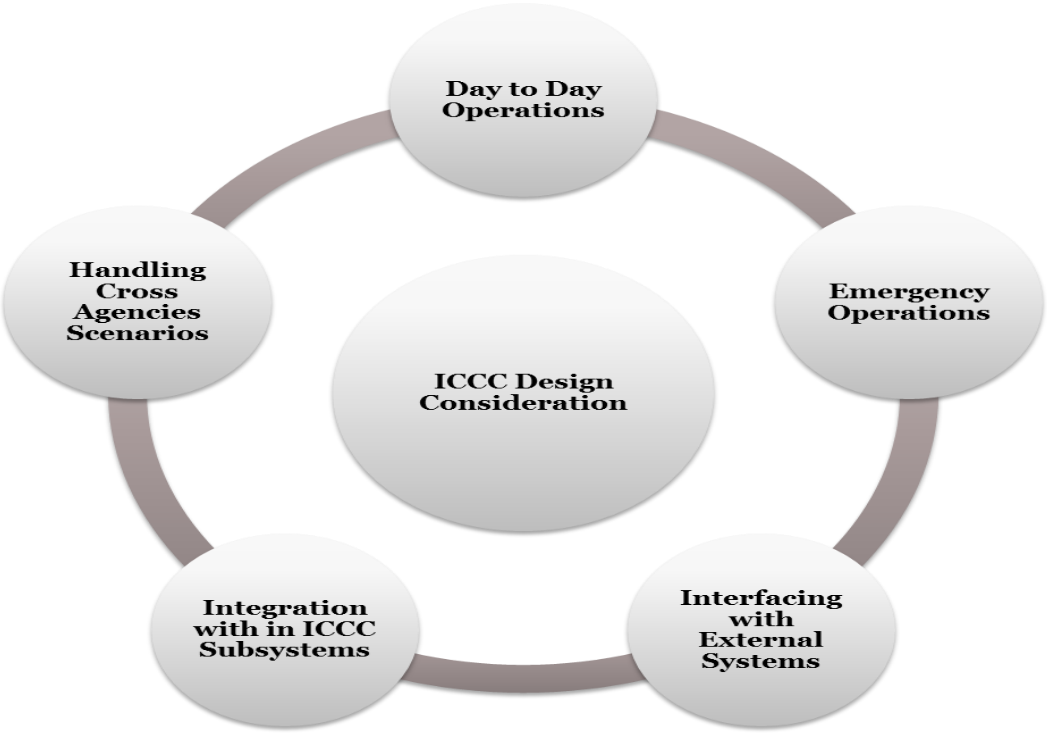
a. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices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

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

4.1 Characteristics of design

While designing the Integrated Command and Control Centre (ICCC), the key aspects to be considered are:

- Real time integration with other systems within the ICCC
- Interface with systems of other agencies e.g. Police CAD system with emergency response
- Handling cross agency scenarios including police, traffic and utilities
- City Management Activities in in routine day to day as well as emergency scenarios


Day to Day Operations
Emergency Operations
Interfacing with External Systems
Integration with in ICCC Subsystems
Handling Cross Agencies Scenarios
ICCC Design Consideration

4.2 Design Parameters

The Command and Control Centre (CCC) solution has been designed taking into consideration the following key functional parameters –

1. The CCC shall provide for **collaborative monitoring and management** of city operations across various agencies. Accordingly, the CCC solution should provide for real time as well as offline collaboration between the agencies. For e.g. the CCC solution provides for seating space at city operations room for representatives from agencies as well as automated transfer of

relevant data to the agencies for them to take appropriate actions. The design provides for seating capacity of maximum 2 representatives from each of the following departments

a. Police

b. Traffic

c. Electricity

d. Water & Sewerage

2. The ICCC shall need to operate in a 24 X 7 mode

3. Open Standards based interfaces so that additional requirements that might emerge in the future can be easily accommodated without requiring for a major change in the solution architecture

4. Cater to the common data requirements of other applications. For e.g. the CCC shall provide for common GIS layer that would be used by all applications needing GIS functionality

5. Act as single point of contact for citizen interface by attending to voice calls as well as attending to their complaints registered through other channels including web, smart mobile applications.

6. ICCC shall define the Standard Operating Procedures (SOPs) that would be followed for managing and tracking the incidents. These SOPs shall be able to be further refined through the data analytics being performed in the CCC.

7. ICCC shall be enabler to deal with any cyber security issue as per the guideline published under the 12th (5 year plan) on Cyber Security as a sub group of Information technology. Refer **Annexure -1**.

4.3 Elements of ICCC

Integrated Command and Control Centre (ICCC) is the heart of the ICT backbone where the overall monitoring and control of major functions of the data / communication network resides. The actual control of the various systems / subsystems will be done remotely by their personnel housed in the ICCC. The required data for monitoring these system / sub-system operations will be received by the relevant operators handling the respective functions in the Operation Centre.

The ICCC Facility is planned to be implemented in a new facility that will be constructed within the premises of LMC office, Zone-D, Sarabha Nagar and Physical construction of ICCC shall be out of Scope of MSI. This new building will have a dedicated space for housing the ICCC facility. The approach to the ICCC Facility will be based on the following basic tenets:

- Spacing should be provided for teams from different departments
- Design of the City ICCC should be as per the ISO 11064 standards (as per the latest version)

The required data for monitoring these system / sub-system operations will be received by the relevant operators handling the respective functions in the Operation Centre. The different Control Centres envisaged for various functions are:

The following table illustrates the floor area that is being considered in the ICCC facility:

S. No	Expenditure item	Units (area) Sq. Ft.
1	City Operation Room	1,000
2	Meeting Room	250
3	Contact Center Room	150
4	Technical Support Room	150
5	War Room separated with glass glazing	300
6	Electrical room & Utility Room	150
7	Store Room	100
8	Washrooms	100
9	Pantry	150
10	Entrance for telecom component (Fibre cabling etc.)	100
11	Conference Room	250
14	Reception Area	100
15	Data Centre	200
Total Area (Approx.)		**3000**

1. City Operation Center

The ICCC will be the primary work space that service associates and technicians utilize to monitor, manage and troubleshoot problems on critical services, such as; Security Surveillance, Water, Power, Crisis & Disaster Management, Automated Fire Alarm, Emergency Services (Police, Ambulance), Traffic Monitoring, Access Control, Citizen Services, etc.

The ICCC prevents most city service disruptions by providing around-the-clock proactive monitoring of Ludhiana critical functions. The ICCC provides the capability for effective service-based monitoring by clearly identifying services, their related infrastructure and any impact of service breakdown/failure on the business goals of customers.

The ICCC offers oversight of problems, configuration and change management, facility wide security, performance and policy monitoring, reporting, quality assurance, scheduling, and documentation by utilizing centralized management, monitoring and analysis tools. The ICCC provides a structured environment that effectively coordinates operational activities with all participants and vendors.

The ICCC technicians typically provide support twenty-four hours a day, seven days a week. Typical daily processes would include:

- Ensuring continuous operation of servers and services;

- Monitoring operations of all mission critical services and devices;
- Providing quality support for facility wide system users;
- First line troubleshooting of all mission critical service related problems;
- Tracking and documenting resolution of problems; and
- 24 hours a day, 7 days a week supervised operation by highly specialized personnel.

The ICCC area houses Operation Centre staff consisting of Operations and maintenance staff for various ICT services such as CCTV surveillance, Signage, ITMS, SCADA, GIS, , Parking management, Asset management, and various call centres staff for city-wide services such as Police, Fire, Ambulance, etc.

A Video Display Wall envisaged with 9 nos. of cubes placed adjacent to each other and each of the clusters with 3x3 LED Panels/ screens. The screens selected shall be full HD LED panels/screens, with associated video wall controller, display software with edge blending feature.

2. Situation Room/War Room

The other part of ICCC consists of one Situation Room separated by a glass wall, In the event of a crisis situation(s), the Situational Room will provide all the technology support to the key decision makers make their decisions. This will include IP phone connectivity, Projector and LED screens, desk mikes etc.

3. Meeting Rooms

There will be a provision for meeting rooms for the ICCC teams to conduct regular discussions and collaborate on a regular basis. The meeting rooms will be equipped with LED Screen and IP Speaker phones to provide a conductive environment for meetings.

4. Conference Room

Considering that the ICCC will be central monitoring system of the entire city, it will also be the nerve centre of handling city-wide incidents that requires collaboration from different departments. In the event of a city-wide incident, the Conference Room will be used to brief the press/media on the developing situation.

5. Contact Centre/ Help Desk

The Contact / Call Center will log and track all tickets raised either by voice call, email, SMS, web requests through portal, in-person requests, etc. All tickets shall be tracked and automatically brought-up for necessary actions until final resolution, tracking or escalation. The CC will house voice and data telecommunications services, automatic call distribution equipment and other related system technologies.

The ICCC will provide services for the city-wide callers for complaints related to the Utility services, Municipal services and other planned citizen services and also handle calls for emergency services related to Police, Fire and Ambulance services. The exact operating model and nature of work for the CC will be defined in the CONOPS developed by the MSI.

6. Secured Data Centre

The Secured Data Center will be used to house active equipment like Application Servers, Ethernet switches, IP communications network, etc. From a logical perspective, Data Center will be hosting all the Application Servers for; CCTV Video surveillance, ITMS, Access Control /Authentication etc.

The Secured Data Center (SDC) will be serving the communications and services needs of the whole of Ludhiana City. Concurrently, maintainable site infrastructure with expected availability of 99.982% is to be established along with multiple independent distribution communication paths serving the IT equipment and duct at Entrance Facility). All IT equipment will be dual-powered and fully compatible with the topology of the site's architecture.

7. Data Centre Grounding/Earthing Considerations

The grounding system for the DC is not just a protection against a lightning strike. It is an active, functioning system that provides protection for personnel and equipment. Proper grounding is essential for efficient system performance. Surges that are not properly dissipated by the grounding system introduce electrical noise on data cables. They cause faulty data signals and dropped packets, thus decreasing the throughput and overall efficiency of the network.

The purpose of the grounding system is to create a low-impedance path to earth ground for electrical surges and transient voltages. Lightning, fault currents, circuit switching (motors turning on and off), and electrostatic discharge are the common causes of these surges and transient voltages. An effective grounding system minimizes the detrimental effects of these surges.

8. Data center grounding is governed by following standards

TIA-942, Telecommunications Infrastructure Standard for Data Centres - TIA-942 defines practical methods to ensure electrical continuity throughout the rack materials and proper grounding of racks and rack- mounted equipment. This is the only specification that addresses problems specific to data centre infrastructure.

ISO 27001 – ISMS: The Datacenter should comply with ISO 27001 – ISMS guideline provided by International Organization for Standardization. This standards helps organizations keep information assets of the Datacenter secure.

All information held and processed by datacenter is subject to the risks of attack, error and natural disaster, and other vulnerabilities inherent to its use. Information security is therefore at the heart of an organization's activities and focuses on information that is considered a valuable "asset" requiring appropriate protection, for example against the loss of availability, confidentiality and integrity. Providing a model to follow when setting up and operating a management system.

9. Entrance Facility Room

- The Entrance Facility shall host IP NGN Core, Distribution and Aggregation network (active) equipment for following networks & services:
  - Public safety & security Surveillance System,
  - Traffic management system (ITMS),
  - Engineering SCADA Network,
  - Wi-Fi Backbone,
  - Smart City Services such as e-governance, municipal services, educational Services, health care services and Tele presence.

- The Entrance Facility co-located with ICCC as a combined facility shall also provide facility for landing of services & hosting of IP NGN Core, Distribution and Aggregation network (active) equipment for 4- 5 TELCO's licensed to provide ISP services in Ludhiana city.

- The Entrance Facility will also host the fiber optics backbone and distribution links, fiber optical distribution Frames (ODFs) as well as cable patching systems;

- It may also host optional IP Access active equipment to support localized services like Traffic Management, Digital Signage, Video Surveillance, etc.; sufficient space and MEP provisions shall be included in the design to accommodate this.

The Entrance Facility shall also have suitably designed environmental conditions including cooling, humidity, air flow, power distribution, UPS, raised floor, cable containment systems

10. Technical Support Room

Technical support room will have a sitting arrangement of various technical staff who will be responsible for providing technical assistance during operation stage of the ICCC.

Following Technical experts would be providing services:

S. No	Manpower	No. of Resources	No. of Man Months	Remarks
During Implementation Phase				
1	Project Manager	1	09	Full Time
2	Solution Architect	1	05	Intermittent
3	Data / Command Centre Expert	1	05	Intermittent
4	Network Architect	1	05	Intermittent
5	Security Infrastructure Specialist	1	05	Intermittent
6	Server Storage / Database Expert	1	06	Intermittent
7	GIS Expert	1	04	Intermittent
8	IBMS Expert	1	05	Intermittent
9	Electrical Engineer / Specialist	1	05	Intermittent

S. No	Manpower	No. of Resources	No. of Man Months	Remarks
10	Field Support Staff	6	09	Full Time
11	Non IT Experts	3	09	Full Time
12	Electrical and Plumbing Resource	1	08	Intermittent
13	Security Staff	3	09	1 resource in each shift
14	Housekeeping Staff	1	09	Full Time
15	Admin & Support	1	09	Full Time
During O & M Phase (4 years)				
1	Project Manager	1	48	Full Time
2	Solution Architect	1	24	Intermittent
3	Data / Command Centre Expert	1	24	Intermittent
4	Network Architect	1	24	Intermittent
5	Security Infrastructure Specialist	1	48	Full Time
6	Server Storage / Database Expert	1	48	Full Time
7	GIS Expert	1	24	Intermittent
8	IBMS Expert	1	24	Intermittent
9	Application Analyst	1	24	Intermittent
10	Contact Center Manpower	12	48	4 resources in each shift
11	Field Support Staff	3	48	1 resource in each shift
12	Operators	48	48	16 resources in each shift
13	Non IT Experts	1	48	Full Time
14	Electrical and Plumbing Resource	3	48	1 resource in each shift
15	Security Staff	3	48	1 resource in each shift
16	Housekeeping Staff	3	48	1 resource in each shift
17	Admin & Support	1	48	Full Time

4.4 Strategy for Business Continuity

The major objective of having Disaster Recovery Site (DRS) for the ICCC is to ensure reliable Data Backup and provide Periodic Replication solution for the ICCC and DC. The following section describes a broad level strategy for effective recovery of all critical IT applications in a swift and seamless manner and to mobilize all resources of ICCC in terms of People, Process, and Technology, for DR.

Assumptions:

- DR site can be hosted at the SDC on a cloud based model and as per the define SLA between MSI and SDC
- All ICCC Software Applications in the scope of Disaster Recovery are assumed to be critical to ICCC's operations.

- Plan has been envisaged for ICCC personnel and systems to be prepared for the worst case scenario in terms of maximum damage owing to the disaster.
- The identified DR Site has all the requisite Hardware and Software availability for DR.
- All key personnel shall be available immediately, in the event of a disaster, so as to perform the allotted duties accordingly. In addition, all User Department / ICCC vendors will perform according to their commitments for support of ICCC during a disaster.
- All critical data required for Disaster Recovery is readily available.
- Procedures for back-up and off-site storage of computer media and documents should be followed.
- Critical Third-party resources listed in the DR Plan are available from identified suppliers or off-site storage facilities.
- The Disaster Recovery Plan will serve as a set of guidelines, not absolute rules. It is not all-inclusive.

Decisions not expressly documented within, are to be made by the Crisis Management Team/ Disaster Recovery Team during the recovery process.

Not every Security breach is a Disaster, and not every Power outage a reason to declare a Disaster. Following are the Disaster exclusions, i.e., events that do not qualify to invoke a Disaster Recovery scenario:

- Known Data Center equipment malfunctioning, where procedures and guidelines are already known to ICCC on the recovery of the same.
- Any event covered under the Prevention Strategies/Fault Tolerance at ICCC.
- Network spikes caused owing to high traffic flows and not due to any equipment / Software issues.
- Resignation / extended unplanned Leave of any Data Center employee, however critical he / she may be to the daily Data Center operations.
- Virus / Spamming attacks on a single Server causing an isolated application outage.
- Any non-critical application shutting down, irrespective of the down time duration
- Planned Individual critical DR application shut down for a period less than the Defined DR RTO (Recovery Time Objective).
- Natural Calamity in the neighboring areas not bound to affect Data Center premises / operations.

Broadly, **threats** that are bound to affect any ICCC have been defined below:

- Fire/ Explosion
- Earthquake/ Floods

- Power Outage
- Air Conditioning Failure
- Political/Civil Unrest/ Internal Strikes
- Theft
- Lightning/ Heavy rains/ Storms
- Pests
- Vendor Support Failure
- Bombing
- Virus attack
- Denial of Service
- Network Penetration/ Internal- External Hacking
- WAN Link Failure
- Hardware Failure
- Software Failure, etc.

A number of scenarios may exist for ICCC that may be potentially fatal for Disaster Declaration, caused by Threats as mentioned above. These impacts are bound to cause disruptions to the functioning of the ICCC in terms of People as well as the IT Infrastructure placed at the ICCCs. A Disaster, thus, may be defined through the context of these disruptions.

Intensity of Disaster

LEVEL	DESCRIPTION
LEVEL 1	**Failure impacting single Department** Significant malfunction of/disruption to primary infrastructure supporting operations of a single System. e.g., Application failure
LEVEL 2	**Failure impacting multiple Departments** Significant malfunction of/disruption to critical primary infrastructure, supporting operations of multiple Systems. For e.g., failure of any of the critical primary servers or data storage systems
LEVEL 3	**Premises unavailable** Total shutdown of office infrastructure, as a result of fire, building collapse, bomb explosions etc. since the premises and equipment are inaccessible, people may have to congregate at an alternate location, if required.
LEVEL 4	**Citywide disaster**

LEVEL	DESCRIPTION
	Major impedance to employees trying to reach office or alternate office resources - e.g. due to riots, floods or other major citywide catastrophe.

It is recommended to have Cloud based DR site with following Replication capabilities:

Replication is the process of sharing information so as to ensure consistency between redundant resources, such as software or hardware components, to improve reliability, fault-tolerance, or accessibility. Data Replication is chosen if the same data is stored on multiple storage devices, and computation replication is chosen if the same computing task is executed many times. A computational task is typically replicated in space, i.e. executed on separate devices, or it could be replicated in time, if it is executed repeatedly on a single device.

There are primarily three types of standard replication methodologies as described below:

1. Storage Based Replication

There are two Storage Replication techniques available in the industry today, as follows:

a. RDBMS based Replication:

City will be having Databases with inbuilt capacity for replication, like Databases using Oracle Data Guard. In such a scenario the requirement of each database will be different and it will be the responsibility of the City to maintain it.

- Database based replication may require installation/configuration licenses of DB
- Database based replication solution typically provides support for replicating across storage models from different vendors.
- This may need to be procured from the same DB vendor as of the DB licenses of the application.

b. Appliance Based Replication

In appliance based replication, an independent appliance is being installed, which would be utilized for sending and replicating data from main site to remote site without **de duplication** of the data by. Appliance based replication method will help replicating data based on capacity optimization.

The local node within a local domain communicates with nodes of remote domains in a system through a communication network. Each domain has its own distributed hash table that partitions key space and assigns a certain key range to an owner node within the domain. For new data, the local node queries owner nodes of domains in the system progressively from the local domain to remote domains for a duplicate of the new data. Depending on a result returned by owner nodes and factors for replication strategies, the local node determines a replication strategy and records the new data in the local node pursuant to the replication strategy

Following are the points to further elaborate the solution pointers:

- Appliance based replication requires installation/configuration of some components at servers/ storage array.
- Appliance based replication solution typically provides support for replicating across storage models from different vendors.
- Appliance based replication software supports IP protocol natively and does not require any external FC-IP conversion equipment.
- This capability may not be provided by the Storage vendor natively and may need to be procured from a different vendor.
- The licensing methodology is typically based on the amount of data that needs to be replicated. It is typically independent on number of servers that access the data in the attached storage array.
- This methodology may entail utilization of server/storage resources for its functioning. Typically, the appliance will also need to be sized appropriately based on the expected workload.
- It supports replication in both synchronous as well as asynchronous modes, which can be configured as per the requirements and feasibility of the solution.
- This methodology supports different topologies like one to one, one to many. However, the extent of support for these topologies maybe vendor dependent
- Certain features and capabilities of appliance based replication may be vendor specific.
- This methodology supports multiple type of application with the same solution.
- In storage based replication, the data is being replicated to the remote site with the help of software being run at the storage itself.

2. ***Host Based Replication***

The Servers, whose data needs to be replicated, act as a host and run the replication software to replicate data across sites. Following points would further elaborate:

- Host based replication requires installation of replication solution across all the servers whose data needs to be replicated. This data might be in an external storage array or internal to the servers.
- Host based Replication solution typically provides support for replicating across storage models from different vendors.

- Host based replication software supports IP protocol natively and does not require any external FC-IP conversion equipment.
- This capability may not be provided by the Storage vendor natively and may need to be procured from a different vendor.
- The licensing methodology is typically dependent on the number of servers. It is independent on amount of data that needs to be replicated.
- This methodology may entail utilization of server resources for its functioning.
- It supports replication in both synchronous as well as asynchronous modes, which can be configured as per the requirements and feasibility of the solution.
- This methodology supports different topologies like one to one, one to many. However, the extent of support for these topologies maybe vendor dependent
- Certain features and capabilities of host based replication may be vendor/ storage specific.
- This methodology supports multiple type of application with the same solution.

3. *Application Based Replication*

Application based replication essentially consists of having an application with its own data replication capability, which shall be utilized for replicating data from main site to remote site. Below points would further help in defining the same:

- Application based replication may require installation/configuration of some components on the servers.
- Application based replication solution typically provides support for replicating across storage models from different vendors.
- Application based replication software

This capability may not be provided by the Storage vendor natively and may need to be procured from the application provider. The licensing methodology is typically dependent on the number of servers. It is independent on amount of data that needs to be replicated. This methodology may entail utilization of server resources for its functioning. It supports replication in both synchronous as well as asynchronous modes, which can be configured as per the requirements and feasibility of the solution. This methodology supports different topologies like one to one, one to many. However, the extent of support for these topologies may be application vendor dependent. Certain features and capabilities of application based replication may be application specific.

The capability of application based solution with respect to data replication is restricted to a specific application only. This means that each application will have its specific replication methodology which will not support any other application.

4. Key Considerations while choosing a Replication Solution

There are a number of factors which shall help in understanding the requirements and identifying the appropriate solution. The parameters, as being mentioned below, may vary from application to application or environment to environment and hence, it becomes further important to delve on these and come out with an appropriate solution:

a. **Recovery Point Objective / Recovery Time Objective:** Recovery Point and Time Objectives define the criticality of the data and acceptable level of the application unavailability. This becomes one of the most prominent factors for identifying the appropriate replication methodology.

b. **Amount of data:** The rate of data change would further becomes a parameter which determines the identification of solution, as there may be a requirement of architectural enhancements to be done based on the data change rate and hence, feasibility of the appropriate solution also needs to be examined for the same

c. **Number of servers:** Number of servers may define the choice of replication solution again, as this would be a determination factor in understanding the manageability of the complete environment.

d. **Interoperability:** Choice of replication solution becomes even more difficult and important in very complex environments, involving different type of storage platforms. The replication solution required in such environment should be able to work as an independent platform for replication of data across different heterogeneous storage

e. **Cost:** The choice of technology and solution is also being limited with respect to the cost associated with the solution. There may be a solution, becoming unviable because of the cost of the components involved and licensing required to implement the entire solution

f. **Support:** The choice of solution also needs to be identified in relation to the availability and kind of support available for the same. It becomes important to have a solution which is fully supported by the vendor, as per the requirements of the DR replication technology, so as to meet the overall objectives of uptime of entire solution.

4.5 Exclusions

The following actionable will not be a part of the scope of System Integrator:

The System integrator will not be responsible for creation of any physical infrastructure to the Integrated Command and Control Centre.

Design, Procurement, Construction, Testing and Commissioning of

- CCC Facility Physical Build
- Electrical and Mechanical Components
- Electrical Distribution Room

4.6 Layered Protocol Matrix – ICCC

Layers	Physical Connectivity	Network Protocol	Data Inter-exchange Protocol
Application Layer	USB, RS 232, Ethernet port, Wi-Fi	FTP, SMTP, DNS, TFTP, SNMP	HTTP, POP3, TCP/IP
Management Layer	USB, RS 232, Ethernet port, Wi-Fi	TCP, UDP, DCCP, SCTP	TCP/IP, UDP
Network/Middleware Layer	USB, RS 232, Ethernet port, Wi-Fi	ARP, RIP, EIGRP, IGRP, IPv6, IPv4, IP Sec	Ethernet Protocol, TCP/IP
Data Collection/Update Layer	USB, RS 232, Ethernet Port	DTP, IEEE 802.11, PPP, PPTP, STP, VTP, VLAN,TCP	Wiegand, TCP/IP, RS 485
Sensor Layer	Wired Communication, RS 485, USB, RS 232, Wi-Fi	Zigbee, Z-wave, Dali, DSL, ISDN, 10BASE-T, IEEE 802.3, Bluetooth, LoRa, NBIoT, MQTT	Wiegand, TCP/IP, RS 485, Modbus, Lonbus , BACnet, Wired communication,, UDP/IP (unicast, multicast IGMP),ONVIF, ICMP, IPv4, IPv6, SNMP v2c/v3, HTTP, HTTPS,SSL, SSH, SMTP, FTP, RTSP, UPnP, DNS, NTP, RTP, RTCP, LDAP (client), QoS, GB28181

4.7 Integrations

For successful integration it is required to have protocol and component level compatibility between existing control centres and the envisaged command and control centre in order to have one uninterrupted operating picture of the city at CCC.

The solution implemented will be scalable across all future integrations and demands that arise for technology solutions of LSCL that will augment to the city wide network of sensors.

City services such as Utilities, surveillance, parking, environmental parameters, self-service kiosks, smart meter and ITMS which will act either as upstream or downstream interfaces to the Integrated Operations Platform will have compatible APIs to integrate with CCC.

- Systems reporting on public safety issues.
- Systems reporting on traffic events.
- Systems reporting on water quality and usage.
- Systems providing data on outages and status of related work orders.

The following sections details out the status of systems which are envisaged for integration with the Command and Control Centre:

1. **Services envisaged to be ready before the implementation of Integrated Command and Control Centre**

S. No.	Modules	Present Automation Status	Planned Automation in next 1 years (Near Future Integration)
1	Smart Lighting	No	Yes
2	Solid Waste Management	Partial	Yes
3	Smart Traffic	Partial	Yes
6	City Surveillance	Partial	Yes
7	Smart Governance	Yes	Yes
8	Smart Parking	No	Yes
9	Sewerage	Partial	Yes
10	Power SCADA	Partial	Yes
11	GIS	No	Yes

2. **Services envisage to be ready in future:**

S. No.	Modules	Present Automation Status	Planned Automation in next 1 years (Near Future Integration)	Future Integration
1	Water SCADA	No	No	Yes
2	Health	No	No	Yes

3	Education	No	No	Yes
4	Storm Water Drainage	No	No	Yes
5	City Bus ITMS	Partial	No	Yes

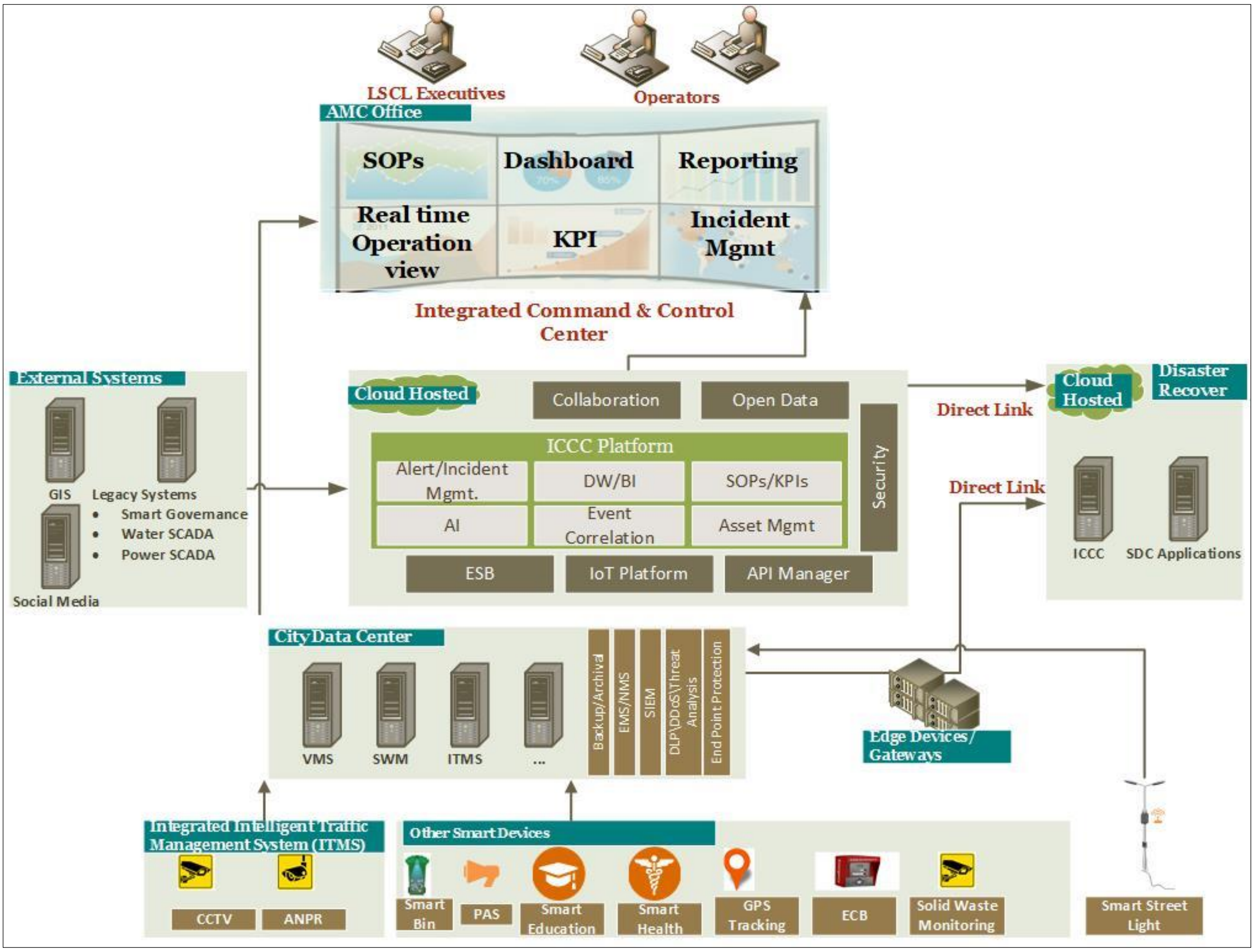
3. Services envisage to be ready along with ICCC as part of MSI Scope

S. No.	Modules	Present Automation Status	Future Integration
1	Panic Button & Emergency Call Box	No	Yes
2	Public Addressal System	No	Yes
3	Environmental Sensors	No	Yes
4	Digital Variable Messaging Display	No	Yes
5	CCTV Cameras	No	Yes

5. Architecture and Solution Elements

5.1 Functional Block Diagram of the Proposed Solution

The interaction of various entities with the various functions of the City Management Center is given in following diagram:

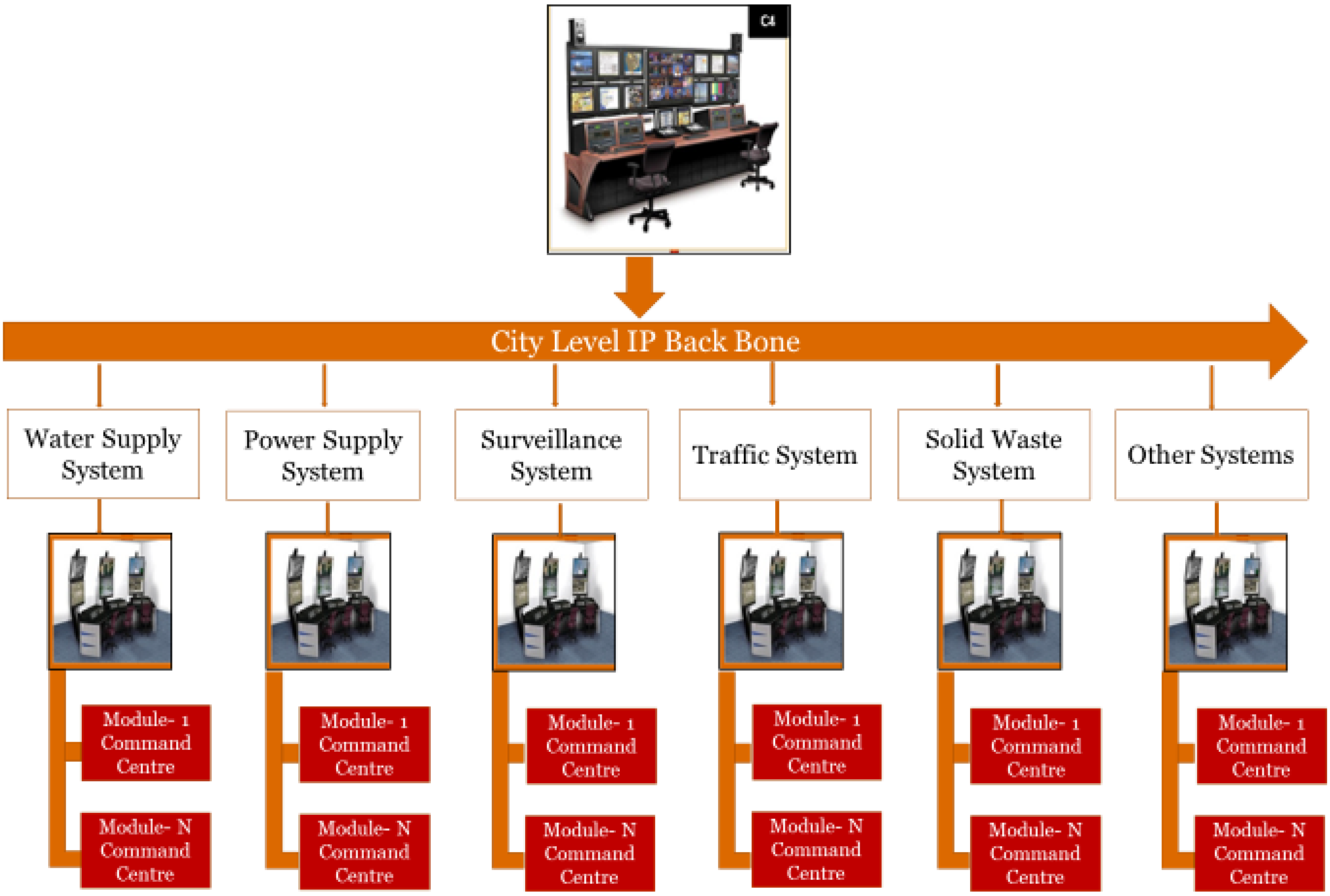


In addition to the above mentioned Components depicted in the Diagram, Command and Control Center building shall be equipped with following facilities:

- An Integrated Building Management System (IBMS)
- Operating facilities for following personnel in the city operations room
  - Contact Center
  - Operators
  - Municipal Staff
  - Supervisors
  - Police representative
  - Traffic police representative

  - Water and sewerage department representative
  - Electricity department representative
- Administration Staff seating
- Equipment room for housing local equipment
- IT support and help desk
- Meeting / conference rooms

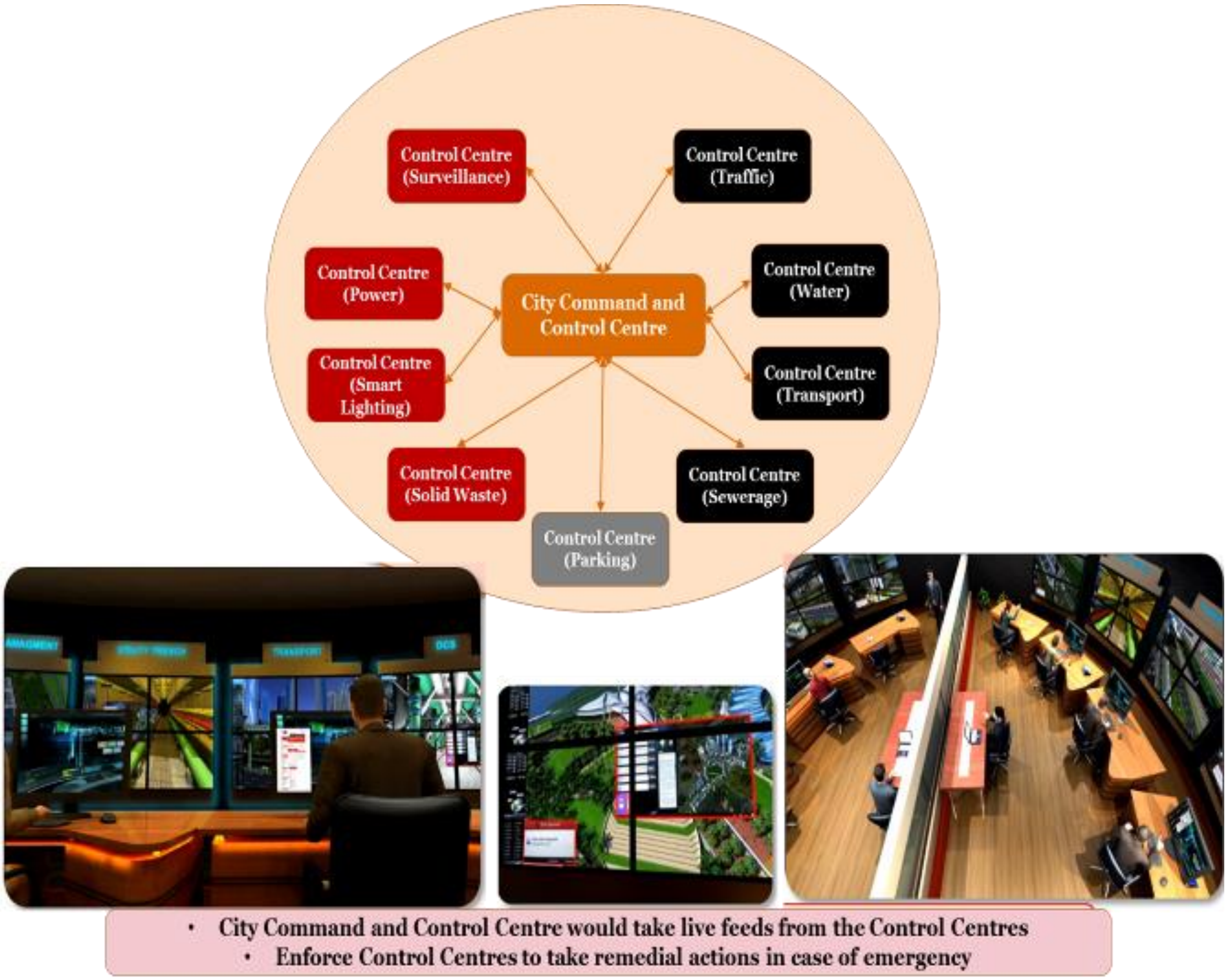
5.2 System Architecture



Summary of System Architecture

- There will be a Central Command and Control Centre connected with IP backbone through OFC cable
- The control centre of the respective modules i.e. surveillance, traffic, sewerage, transport, parking etc. will be connected to the Central Command and Control Centre and giving real time information for monitoring purpose
- Control Centres will be connected with various field level sensors, actuators and controllers

Illustrative image of the Central Command and Control Centre


Control Centre (Surveillance)
Control Centre (Traffic)
Control Centre (Power)
City Command and Control Centre
Control Centre (Water)
Control Centre (Smart Lighting)
Control Centre (Transport)
Control Centre (Solid Waste)
Control Centre (Sewerage)
Control Centre (Parking)

- City Command and Control Centre would take live feeds from the Control Centres
- Enforce Control Centres to take remedial actions in case of emergency

5.3 Functional Requirements

1) CCC shall facilitate the viewing and controlling mechanism for the selected field locations in a fully automated environment for optimized monitoring, regulation and enforcement of services. The CCC shall be accessible by operators and concerned authorized entities with necessary authentication credentials.

2) Various smart elements are able to use the data and intelligence gathered from operations of other elements so that civic services are delivered lot more efficiently and in an informed fashion.

5.3.1 Functional Specifications of the CCC Application Software

Various functional requirements of the CCC application System are given in the table below:

S. No.	Parameters	Minimum Specifications
1	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products.
		Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.
		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion.
		System must provide a comprehensive API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration with existing systems, and future application and sensors which will be deployed on the field.
		The solution should be network and protocol agonistic and provide option to connect legacy system through API's with either read, write or both options. It should connect diverse on premise and/or cloud platform's and make it easy to exchange data and services between them.
		The system shall allow seamless integration with all of the department's existing and future initiatives
		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.
		The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers
2	Convergence of Multiple feeds / services	System need to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases.
		System should support DDE and OLE for integration with Process control systems and sensors
		System should have capability to source data from various systems implemented in Ludhiana City to create actionable intelligence

S. No.	Parameters	Minimum Specifications
3	Industry Standards for the Command & Control Center	The solution should adhere to the Industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility
		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management
		Geo Spatial Standards like GML & KML etc.
		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
4	Command & Control Center Components	Web server to manage client requests. Client should provide web-based, one-stop portals to event information, overall status, and details. The user interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards.
		Application server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide the contacts and instant messaging service to enable effective, real-time communication. It should provide business monitoring service to monitor incoming data records to generate key performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. The application server should provide security services that ensure only authorized users and groups can access data.
		System Platform – The platform should provide a common data integration layer which can collect and contextualize information from disparate data sources regardless of protocol. The platform should support templatization to allow “build once-deploy everywhere” functionality.
		Workflow and Incidents Lifecycle engine – This function should allow users to define and modify new worflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. Workflow approvals should have facility to approve from any device with e-signature. This function should provide facility to trigger a corrective action workflow and define the stakeholders for the same. Should manage the life cycle of incidents and related entities via pre-define workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention.

S. No.	Parameters	Minimum Specifications
		Incidents Planning – should manage the planning preparations of an incident including resource allocation, tasks management etc.
		Analytics and MIS – should provide users with business analytics reporting and tools to organize, evaluate and efficiently perform day to day operations
		Security & Roles – should manage roles definition for internal as well as external access
		Centralized data archiving for operational data : Should provide facility for centralized storage of operational data (time-series or transactional) with high granularity and data compression capability
		Mobility: should enable app-based access to monitor alerts, KPI ,KOPs, SOPs and reports to mobile users. Should support popularly user's smartphone /tablets. App content should be presented in context to the user role.
5	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:
		Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.
		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention.
		Should support for multiple incidents with both segregated and/or overlapping management and response teams.
		Should support Geospatial rendering of event and incident information.
		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.
		Should support incorporation of resource database for mobilizing the resources for response.
		Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.
		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems
		Should provide detailed reports and summary views to multiple users based on their roles.

S. No.	Parameters	Minimum Specifications
		A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.
		Provide User-defined forms as well as Standard Incident Command Forms for incident management.
6	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance
		Collects major information from other integrated City sensors/platforms.
		Should allow different inputs beyond cameras, such as, PC screen, web page, and other external devices for rich screen layout
		Multi-displays configurations
		Use of, GIS tool which allows easy map editing for wide area monitoring (Google map, Bing map, ESRI Arc GIS map, etc.).
		Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command center
		Should provide historical reports, event data & activity log. The reports can be exported to pdf or html formats.
		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
7	Integration with Social Media & Open Source Intelligence	Should provide integration of the Incident Management application with the social media. Should Provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.
		Should extract messages and display it in an operational dashboard.
		Should be able to correlate the extracted message from the social media with existing / other events and then should be able to initiate an SOP.
		Should be able to identify the critical information and should be able to link it to an existing SOP or a new SOP should be started.
		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.

S. No.	Parameters	Minimum Specifications
8	Device Status, Obstruction Detection and Availability Notification	Should provide icon based user interface on the GIS map to report non-functional device.
		Should also provide a single tabular view to list all devices along with their availability status in real time.
		Should provide User Interface to publish messages to multiple devices at the same time.
9	Event Correlation	Command & Control Center should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.
10	Standard Operations Procedures (SOP)	Command & Control Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.
		The users should be able to edit the SOP, including adding, editing, or deleting the activities.
		The users should be able to also add comments to or stop the SOP (prior to completion).
		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
		The SOP Tool should have capability to define the following activity types:
		Manual Activity - An activity that is done manually by the owner and provides details in the description field.
		Automation Activity - An activity that initiates and tracks a particular work order and selected a predefined work order from the list.
		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
		Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
		SOP Activity - An activity that launches another standard operating procedure.

S. No.	Parameters	Minimum Specifications
11	Key Performance Indicator	Command & Control Center should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.
		Green indicates that the status is acceptable, based on the parameters for that KPI, no action is required.
		Yellow indicates that caution or monitoring is required, action may be required.
		Red indicates that the status is critical and action is recommended.
12	Reporting Requirements	Command & Control Center should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup
		The solution should generate Customized reports based on the area, sensor type or periodic or any other customer reports as per choice of the administrators
13	Collaboration Tools	Should provide tools for users to collaborate & communicate in real-time using instant messaging features.
14	Communication Requirements	The solution should adhere to the below mentioned communication requirements.
		Provide the ability to search/locate resources based on name, department, role, geography, skill etc. for rapidly assembling a team, across department, divisions and agency boundaries, during emergency
		Provide the capability to Invite - Using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.
		Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E- mail and Social Media
		The solution should provide Dispatch Console integrates with various communication channels. It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams. It should assess the common operating picture, identify & dispatch mobile resources available nearby the incident location. Augment resources from multiple agencies for coordinated response.
15	Authentication	Use authentication information to authenticate individuals and/or assign roles.

S. No.	Parameters	Minimum Specifications
16	Instant messaging	Provide ability to converse virtually through the exchange of text, audio, and/or video based information in real time with one or more individuals within the emergency management community.
17	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command & Control Center. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the Command & Control Center, the event should be displayed on an operations dashboard and analyzed to determine a proper directive.
		Directives issued by the Command & Control Center should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.
18	What-if Analysis Tool	The solution should provide the capability to manage the emergencies and in-turn reducing risks, salvaging resources to minimize damages and recovering the assets that can speed up recovery.
		To take proactive decisions that help minimize risks and damages, the solution should provide Analytical as part of the Decision Support System. The solution should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy to use Graphical User Interface. When in What if Analysis mode the solution should highlight not only the primary asset impacted but also highlight the linked assets which will be impacted. The user should be able to run the What-if Analysis mode for multiple types of emergency events such as Bomb Blast, Weather events, Accidents etc.
19	Resource & Route Optimization	The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send large number of messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media.
20	Alert & Mass Notification Requirements	Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Pager, Voice mail, E-mail and Social Media

S. No.	Parameters	Minimum Specifications
		Provide function for creating the alert content and disseminating to end users. Provision of alerting external broadcasting organizations like Radio, TV, Cellular, etc., as web-service.
		Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.
21	Security & Access Control	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
22	Internet Security	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central repository for administration purposes.
23	Authorization	Should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely
24	User group	Provide policies using separate dimensions of authorization criteria like Traditional static Access Control Lists that describe the principals (users and groups) access to resource and the permissions each of these principals possess.
25	Provide multi-dimensional access control	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
26	Flexible single sign-on (SSO)	Support LDAP authentication mechanism
27	Authentication	Should have ability to respond to real-time data with intelligent & automated decisions
28	Rule Engine & Optimization	Should provide an environment for designing, developing, and deploying business rule applications and event applications.
		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make
		Should have at-least two complementary decision management strategies: business rules and event rules.
29	Situational Awareness COP	The CCA should be able to combine data from various sources and present it as different views tailored to different operator’s needs.

S. No.	Parameters	Minimum Specifications
	(Common Operational Picture)	The CCA should automatically update the information based on alarms and incidents that are presented to it via the business rules engine. The polling and CCA database refresh cycle shall be configurable to match the status of the situation (whether there is an emergency or crisis or just monitoring only).
		Common Operational Picture should comprise of a comprehensive view of the incident or a group of related incidents as on a specific date and time which should include but not be limited to the following:
		✓ Tasks assignment and their status
		✓ Agencies involved
		✓ Resources deployed
		✓ Incident status across relevant parameters of the incident e.g. household affected by a transformer shut down
		✓ Timeline view of the situation
		Suggested actions from the system with their status
30	Task Management	The system should be able to create, assign, track and report on the lifecycle of tasks during a particular incident.
		The system should allow a particular task to be decomposed into sub-tasks.
		The system should provide an easy to interpret management dashboard view of the progress of all tasks during an incident.
		The system should be able to organise the visual representation of tasks into prioritized list, filtered list, as well as colour coded representation for ease of understanding.
		The system should be able to perform the following functions around task management:
		✓ Create a task with unique ID. (Subtasks shall follow parent ID with second level numbering).
		✓ Assign a target completion date and time for the task, either directly or as a time-span from the task's creation.
		✓ Date and time stamp of the creation of the task.
		✓ Log and track status of tasks. System should provide capability to define status of tasks during its lifecycle. These status definitions could be mapped to other task attributes such as the task type.
		✓ Key-word search against task list.
		The above attributes shall be colour coded.

S. No.	Parameters	Minimum Specifications
		The system shall allow the tasks to be filtered on the real-time dashboard by agency then by task status. This filtering should allow an operator to filter for all tasks of a particular state or a combination of state; and by the time remaining until (or time elapsed since) the target completion time.
		The system should allow multiple individual workstations to select specific agencies of interest on each workstation simultaneously.
		The system should allow the LSCL to display all agencies' tasks simultaneously as well.
		The tasks should be displayed on a real-time timeline.
		The criticality of tasks should be dynamically changed depending on the performance of the incident response.
31	Timeline and Charting	The system should provide a facility to see incidents and actions (tasks) added to the CCA in a tabular list form as well as GANTT chart format filtered by day, week, month, year or any specific date range.
		The system should provide a facility to see incidents, actions and interdependencies between actions in a clear visual graphical manner.
		The system should be able to filter the information based on at least the following parameters:
		✓ Incident information
		✓ Resources information
		✓ Agency type
		✓ Tasks
		Criticality or priority
32	GIS Display	Shall view the environment through geospatial or fixed composite computer-generated (JPEG, BMP, AutoCAD, etc.) map
		Should allow user to view sensor and related name from the displayed map
		Should allow all resources, objects, sensors and elements on the map to be georeferenced such that they have a real world coordinate.
		Should visually display a camera sensor with related camera orientation, camera range and camera field of view angle.
		Should visually display an alarming sensor on map
		Should visually differentiate sensor alarm severities on map through different color and icon identifiers

S. No.	Parameters	Minimum Specifications
		Should immediately view alarm details (including description, video, etc.) and investigate the alarm from the map
		Should allow user to choose camera and other sensors from map to view live video and the data
		Should allow user to choose camera and take live video image snapshot and save to file from any camera
		Should allow user to choose camera from map to move PTZ cameras
		Should allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time
		Should allow user to choose camera and take recorded video image snapshot and save to file or print from any live or recorded video
		Should allow user to jump from one map to the next with a single click of a mouse with map links
		Should allow map information "layers" to be displayed/hidden on items such as –
		✓ Sensor names
		✓ Sensors
		✓ Sensor range (e.g. camera – orientation, range, field of view angle)
		✓ Locations and zones
		✓ Perimeter ranges
		✓ Resource tracks
		Allow user to zoom in/out on different regions of map graphic
33	Video Display	Shall view live or recorded video from resizable and movable windows
		Should have an ability to perform video controls for video systems from workstation
		Shall play, fast-forward, rewind, pause, and specify time to play recorded video
		Shall take a video still image (snapshot) from live or recorded video
		Shall export video for user specified time and duration
		Shall have the capability to move PTZ cameras
		Shall view Video in Video Matrix
		Shall display in 1x1, 2x2, 3x3 and 4x4 window formats

S. No.	Parameters	Minimum Specifications
		Shall enable operator to specify video windows to be displayed in matrix
		Shall enable matrix settings to be saved per user
		Shall view either live or recorded video can be displayed in the video matrix window.
		Shall enable video snapshot to be taken and saved from any window pane in the matrix view
		Shall rotate video in "virtual" video guard tour
		Shall rotate through multiple video views based on predefined video camera sequence and duration.
		Shall enable the user to pause the rotation of video and resume the video rotation again
		Shall enable times between new video to be adjusted
		Shall enable both live video and recorded video to be played through the video guard tour.
		Shall enable alarms to be generated from any video pane
		Shall enable user to only view and control video for which they have been assigned permissions by the administrator
		Shall manually create an alarm from the live or recorded video with specified severity and description
34	Alarm Display	Should have an ability to display alarm condition through visual display and audible tone
		Should have an ability to simultaneously handle multiple alarms from multiple workstations
		Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre-defined parameters such as alarm type, location, sensor, severity, etc.
		Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence
35	Historical Alarm Handling	Should have an ability to view historical alarms details even after the alarm has been acknowledged or closed.
		Should have an ability to sort alarms according to date/time, severity, type, and sensor ID or location.
36	Alarm Reporting	Should have an ability to generate a full incident report of the alarm being generated.
		Should have an ability to display report on monitor and print report

S. No.	Parameters	Minimum Specifications
		Should have details of alarm including
		✓ severity, time/date, description and location
		✓ Captured video image snapshots
		✓ Relevant sensor data such as SCADA sensors
		✓ Response instructions
		✓ Alarm activities (audit trail)
		Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt, and any other formats as per requirement
		Should have an ability to generate an alarm incident package including the full incident report and exported sensor data from the incident in a specific folder location.
37	Alarm Policies and Business Logic Administration	The CCA solution should have the following ability to handle the workflow alarms through graphical user interface.
		Should have an ability to match keywords or text from the alarming subsystem's incident description to raise an alarm using criteria including exact match, exact NOT match, contains match, wildcard match and regularly expression match (such as forced door alarm, denied access, door open too long, etc.)
		Should have an ability to optionally match alarming subsystem's incident status, incident severity, and sensor type
		Should have an ability to apply any alarm policy to one or more monitoring area(s) or zone(s) without having to reapplying the policy multiple times.
		Should have an ability to apply any alarm policy to one or more sensors without having to reapply the policy multiple times.
		Should have an ability to assign specific actions for each alarm
		Should have an ability to activate or deactivate alarms as required
		Should have an ability to create exceptions
		Should Create batch-wise rules and process them
		Should Check and rectify logical errors and contradictory rules
		Should have an ability to schedule execution of rules
		Should Suspend or Terminate the application of rule
		Should archive unused or deactivated rules

5.3.2 Functional Requirement of Citizen Services Mobile Application

The Citizen Mobile Application will serves as a single unified platform for the citizens to engage with the government, avail citizen centric (G2C & B2C services), register municipality related complaints, receive issue resolution, access live city feeds through the city dashboard, learn about governance schemes, projects, and initiatives. The four main components of the planned platform are: Citizen Collaboration, Grievance Redressal, Citizen Service Delivery (G2C & B2C services) and City Dashboard

The Citizen Mobile Application will receive grievances and inputs from both citizen and the Government, using multiple channels (including external social media) to drive the different redressal services, and in turn disseminate information using external media and the platform itself as channels. All the discussion topics, surveys, polls, blogs are specific to discussion groups. Hence, separate Government departments can create and moderate different discussion groups and the discussion topics, surveys, polls and blogs can be created within these discussion groups and moderated by the concerned Government department using the admin console. The solution also boasts of a robust analytical engine, a dedicated team to monitor and update the collaboration platform and LSCL stakeholders about the citizen sentiment/feedback on various discussion topics/polls on regular intervals.

5.3.3 Functional Specifications of non IT components

Proposed specifications for various Non-IT components, required at Command Center and the Edge Level, are given in this section. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command Centers before Go Live.

1. **Civil and Architectural work**

   a. **False Ceiling & Metal Panelling (at Command Center)**

   - Metal false ceiling with powder coated 0.5mm thick hot dipped galvanised steel tiles 595 x 595 mm with regular edge (10mm) suitable for 25mm grid supported on suitable powder coated galvanised steel grid as per manufacturer specification. The same shall be inclusive of cut outs for lighting, AC grills, Fire detectors, nozzles, etc.
   - Control Room wall panelling and ceiling must be 100% modular to accommodate future technological expansions/retrofitting without taking any shut-downs and must be easily replaceable in case of damage.
   - Wall panelling and Ceiling tiles must be a combination of perforated and non-perforated tiles to have Sound absorption coefficient (NRC) value as per ISO:8225-1987, ISO: 354-2003. Panelling to be 100% Modular self inter lockable metal panels of Preformed textured Hot dip galvanized strips and sheets of low carbon steel coated on one side with rigid polyvinylchloride (PVC) film and on the other side a coating based on cross linkable polyester resins (sheet thickness 0.6mm & PVC Coating 0.15mm).
   - Wall Panelling and Ceiling must be seismically tested & certified for Zone 4(Ludhiana) Vibrations. Valid report from government approved test lab to be enclosed with the bid. Control Room Interiors must be free from health hazardous substances because of interior finishes.

- Wall Panelling and Ceiling tiles must be Class A fire rated certified for surface burning characteristics and ROHS certified from to ensure restriction of hazardous substance in any of the materials. This is mandatory to ensure that the materials used in the interiors do not provoke fire. Certificate to be attached with the bid.

- It is imperative that the control centres are designed properly in terms of Aesthetics, Ergonomics and Functionality and should be designed as per ISO 11064 norms .Various aspects should be considered while designing to create ideal work place, considering physiological aspects such as line of sight, field of vision and cognitive factors such as concentration and perceptivity as per ISO 11064

b. **Furniture and Fixture**

- Workstation size of min. 18" depth made with 1.5mm thick laminate of standard make over 18mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish. Edges shall be factory post-formed. The desk shall have the necessary drawers, keyboard trays, cabinets etc. along with sliding / opening as per approved design with quality drawer slides, hinges, locks etc.

- Storage unit with 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the storage of size 1'6"x1'6"x2'4". The same should be provided with all the required accessories including the handle, lock, sliding channel and necessary hardware, etc. complete with French polish

- Cabin table of min. Depth 2' made with 1.5mm thick laminate of standard make over 19mm thick commercial board complete with wooden beading including cutting holes & fixing of cable manager etc. complete with French polish.

- 6" high laminated strip using 1.5mm thick laminate over 10mm thick commercial board on all vertical surface in the entire server & ancillary areas including low height partition, brick wall, partition wall, cladding etc. complete with French polish in all respect.

- Enclosure for gas cylinder of Shutters and Partitions along with wooden support and 18 mm thick MDF board along with 1.5 mm approved laminate colour outside and 2 coat of enamel paint inside the shutter. The same should be provided with all the required accessories including the handle, lock, loaded hinges, tower bolt and necessary hardware etc. complete with French polish.

c. **Partitions** (wherever required as per approved drawing)

- Full height partition wall of 125 mm thick fire line gyp-board partition using 12.5 mm thick double fire line gyp-board on both sides with GI steel metal vertical stud frame of size 75 mm fixed in the floor and ceiling channels of 75 mm wide to provide a strong partition. Glass wool insulation inside shall be provided as required. Fixing is by self-tapping screw with vertical studs being at 610 mm intervals. The same should be inclusive of making cut-outs for switch board, sockets, grill etc. It shall also include preparing the surface smoothly and all as per manufacture's specification etc. finally finishing with one coat of approved brand of fire resistant coating.

- With glazing including the framework of 4” x 2” powder coated aluminium section complete (in areas like partition between server room & other auxiliary areas).
- Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft.) wide.

d. Painting

- Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers’ recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer’s recommendation for coverage of paint.
- For all vertical Plain surface.
- For fire-line gyp-board ceiling.
- POP punning over cement plaster in perfect line and level with thickness of 10 – 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer’s specification.

e. PVC Conduit

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.

- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be hold by steel hooks of approved design of 60cm center the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

f. Wiring

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands permitted at terminations.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indication the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.
- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associate's switch of same capacity. Switch and socket shall be enclosed in a M. S. Sheet steel enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite be connected on the live wire and neutrals of each circuit shall be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.

- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.

g. Earthing

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthen through the cable glands. Earthling shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed.

- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units etc. so as to avoid a ground differential. State shall provide the necessary space required to prepare the earthing pits.

- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.

- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.

- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.

- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.

- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.

- The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.

- A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit needs to be in place for this copper mesh.

- Provide separate Earthing pits for Servers, UPS & Generators as per the standards.

h. Cable Work

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a criss-crossing is avoided and final take off to switch gear is easily facilitated.

- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick 69standard strips and securely fastened to the. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.

- Each section of the rising mains shall be provided with suitable wall straps so that same the can be mounted on the wall.

- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.

- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.

- Necessary earthling arrangement shall be made alongside the rising mains enclosure by Mean of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.

- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

i. Comfort Air Conditioning at Command Centre

- Cooling Capacity as per the requirements at each of the control rooms
- Compressor – Hermetically Sealed Scroll Type
- Refrigerant – R 22 Type
- Power Supply – Three Phase, 380-415 V, 50 Hz
- Air Flow Rate – minimum 19 cu m / min
- Noise Level - < 50 dB
- Operation – Remote Control

j. **Fire Alarm System** Fire can have disastrous consequences and affect operations of a Control Room. The early-detection of fire for effective functioning of the Control Room.

System Description

- The Fire alarm system shall be an single loop addressable fire detection and alarm system, and must be installed as per NFPA 72 guidelines.
- Detection shall be by means of automatic heat and smoke detectors (multi sensor) located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

Control and indicating component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of UL/EN54 Part 2 for the control and indicating component and UL/EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

Smoke detectors – Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of UL/EN54 Part 7. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

- Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.

- Devices shall be compatible with the CIE conforming to the requirements of UL/ EN54 Part 5 the detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.
- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.
- Addressable Manual Call points must also be provided
- Control & Monitor module must be provided for integration with 3rd party systems.

Audible Alarms – Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

Commissioning

- The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

k. Aspirating Smoke Detection System

This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labour necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes.

Codes and standards

- The entire installation shall be installed to comply one or more of the following codes and standards
- NFPA Standards, US
- British Standards, BS 5839 part :1
- IS 11360

Approvals

- All the equipment's shall be tested, approved by any one or more:
- LPCB (Loss Prevention Certification Board), UK
- FM Approved for hazardous locations Class 1,Div 2
- UL (Underwriters Laboratories Inc.), US

- ULC (Underwriters Laboratories Canada), Canada
- Vds (Verband der Sachversicherer e.V), Germany

<u>Design Requirements</u>

- The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.
- It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.
- The system shall allow programming of:

  a) Multiple Smoke Threshold Alarm Levels.
  b) Time Delays.
  c) Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault.
  d) Configurable relay outputs for remote indication of alarm and fault Conditions.

- It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modelling tool.
- Optional equipment may include intelligent remote displays and/or a high level interface with the building fire alarm system, or a dedicated System Management graphics package.
- Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.

<u>Displays on the Detector Assembly</u>

- The detector will be provided with LED indicators.
- Each Detector shall provide the following features: Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector/Smoke Dial display represents the level of smoke present, Fault Indicator, Disabled indicator

<u>Sampling Pipe</u>

- The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.

<u>Installation</u>

- The Contractor shall install the system in accordance with the manufacturer's recommendation.

- Where false ceilings are available, the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.

- Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.

- The bidder shall submit computer generated software calculations for design of aspirating pipe network, on award of the contract.

l. Access Control System

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully operational on line access control system. Access control shall be provided for entry / exit doors. These doors shall be provided with electric locks, and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- Day, Date, Time and duration based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

m. Rodent Repellent

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

• Configuration	: Master console with necessary transducer
• Operating Frequency	: Above 20 KHz (Variable)
• Sound Output	: 80 dB to 110 dB (at 1 meter)
• Power output	: 800 mW per transducer
• Power consumption	: 15 W approximately
• Power Supply	: 230 V AC 50 Hz
• Mounting	: Wall / Table Mounting

5.3.4 Integration Capabilities

1) The CCC will aggregate various data feeds from sensors and systems and further process information out of these data feeds to provide interface /dashboards for generating alert and notifications in real time.

2) The CCC would also equip city administration to respond quickly and effectively to emergency or disaster situation in city through Standard Operating Procedures (SOPs) and step-by-step instructions. The CCC shall support and strengthen coordination in response to incidents/emergencies/crisis situations.

3) Single Dashboard for City Infrastructure Management & Smart City Services for Smart Lighting, Parking System, GIS Services and Other Services of Municipality work visualized real time on 2D/3D map of City. This dashboard can be accessed via web application as well as mobile app. The various information that may be accessed from the system but not limited to are as below:

   - ➢ Visual alerts generated by any endpoint that is part of the city infrastructure e.g. Surveillance cameras, City lights or any other sensors that manages various city management use cases. (integration with existing city surveillance project by Punjab police)
   - ➢ Access information of water management resources (Disaster management cell at Ludhiana will provide the details)
   - ➢ Information about waste management resources
   - ➢ Various citizen services e.g. Land records, Municipality tax, billing etc.
   - ➢ City environmental data
   - ➢ Take action based on events generated by any city infrastructure device

4) 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

5) Sample Use Cases describing the need of integrated systems:

- ***Urban Flooding Scenario**:* The water level sensors (used for flood detection on streets) will send the ambient water levels accumulated on the street to the CCC through the available connectivity. The CCC shall baseline the existing water level and rainfall prediction with erstwhile flood levels to generate an alert for flooding. This alert will then be passed over to the citizens through the variable messaging displays and public address system to warn them of possible flooding in a locality.

- ***Evacuating Hazardous places in event of fire**:* As soon as the Command Center is intimated of a fire through any of the available channels, Fire tenders shall be dispatched to the location along with guidance for shortest path to the accident site. The Fire tender's journey time shall be optimised by providing the best possible green corridor through ATCS (area Traffic Control System). Event trigger shall be also sent to nearest Police Station & nearby hospitals. IP based public address system will be triggered to vacate the nearby fuel stations (if there is any) to reduce the extent of casualty. Information will be passed over trauma centres in the vicinity to prepare for increased number of emergency care patients.

5.3.5 Other Requirements

1) The Integrated Command Control Center will be the nodal point of availability of all online data and information related to various current and future smart elements and will be connected to other LSCL network of services through an integration layer.

2) The CCC will be established with all hardware, software and network infrastructure including switches and routers and will be maintained by the successful bidder throughout the mentioned period. LSCL takes the responsibility of necessary civil work including furniture through another tender process

3) All required Servers, Storage, Software, Firewall, Network Switches for entire project shall be installed in the integrated manner.

4) The controls and displays should be mounted in ergonomically designed consoles to keep operator fatigue to a minimum and efficiency high.

Security: In no circumstances this data accumulated and processed by Command and Control should be compromised. Hence provisions will be made to keep all the data stored in this platform highly secured with required Security framework implementation. The platform will be hosted in Data centre at location decided by LSCL to be provided by successful bidder. Further the platform will provide an open standard based integration Bus with API Management, providing full API lifecycle management with governance and security.

6. Project Management

6.1 Project Prerequisites

The Implementation of the project will have some pre-requisites for its work to begin:

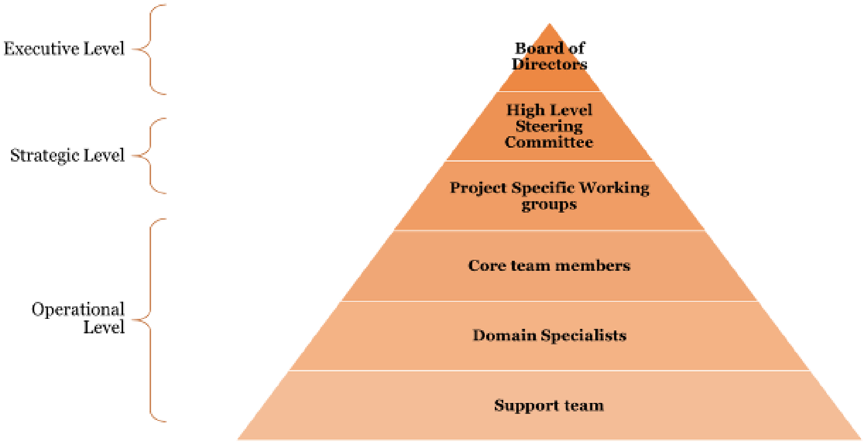
1. The existing safe city command and control centre must be operational and data feeds must be available for the proposed CCC
2. A city wide network based on bandwidth procurement (MPLS network) should be in place connecting existing and proposed ICT infrastructure, and all other control centres and interfacing ICT components
3. The civil infrastructure including physical furniture inside the building must be in place prior to installation of electronics
4. Planning and execution of capacity building and training exercise.

6.2 Project Governance Structure

Project governance is extremely important to be set out at the start of this project. The project governance structure will set out clear responsibility and accountability within the authority for the delivery of the project. It will provide the stakeholders in the authority the ability to manage their interest in the project and support the project implementation team to deliver the required outcomes by providing resources, giving direction and timely decision taking. The governance body will also acts as a forum for any issue resolution and support for information gathering. The effective governance structure would comprise a

- High level steering committee
- Project specific working group
- Quality management committee
- Core team members
- Domain specialists
- Support team

This governance structure would facilitate in streamlining the project activities among each of the team members as per their expertise and skill set as well as ensure the timely delivery of project management tasks and deliverables as required by this engagement.



Executive Level

The **Board of Directors** are at an Executive level focused on resolving strategic budget and resource issues, while the steering committee focusses at a Strategic level, leading the directions and work to be done by highlighting the most pressing issues and questions that the Operational team needs insights to.

The **steering committee** would meet at-least once every month to take important decisions and approvals with the project specific working group and would participate in day to day decision making for the project. The group would also Review the expected outcomes of a project against the realities and monitor expenditures.

Strategic Level

The purposes of the **project specific working groups** on this level is to prioritize deliverables within subject areas, resolve strategic issues, and, on rare occasions, elevate issues as appropriate. These group is also responsible for reviewing the completeness, accuracy, and timeliness of data and deliverables. Output examples include decisions involving complex architectures, designs, network maps, data migrations, solution diagrams and dependency documentation. This group would meet on a weekly basis and, depending on the scope and status of a project and Monitor compliance by proper management processes. The team would also oversee contractors and vendor activity, including any customization/integration of the existing network solution.

Operational Level

The operational level is the most granular, and it usually involves delegates of steering or subcommittee members. This would comprise of core team members, domain experts and support team which could assist in the day to day functioning and execution of the project.

6.3 Project Schedule

The project is envisaged to be implemented within **12 months** upon issue of the Work Order. Operations and management of the entire system including its sub systems, customer support and responsibility as per SLAs for the duration of **4 years post successful implementation**.

List of the broad activities to be carried out by the Systems Integrator and the timelines from the date of Work Order are given in the table below. “D” stands for the date of issue of the Work Order.

Sr. No.	Deliverables	Time Schedule
1	Completion of Scoping and feasibility study (Inception Phase)	D+ 1 Month
2	Installation, Commissioning and Go-Live of ICCC	D+ 3 Months
3	Integration of Smart Features of Phase I	D + 6 Months
4	Submission of SoP’s/KPIs	D + 7 Months
5	Completion of Integration Smart Features and Go-Live (Project Acceptance) – Phase II	D + 9 Months

Sr. No.	Deliverables	Time Schedule
6	Submission of SoPs/ KPIs	D +10
7	Completion of Integration Smart Features and Go-Live (Project Acceptance) – Phase III	D + 12 Months
8	Submission of SoPs/KPIS	D+12 Months

6.4 Project Deliverables

S. No.	Key Activities	Deliverables
Project Inception Phase		
1	Project Kick Off	1. Project Development Plan 2. Risk Management and Mitigation Plan
2	Deployment of manpower	
Requirement Phase		
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification Document 2. System Requirement Specification document (SyRS) 3. Requirements Traceability Matrix 4. Site Survey Report
4	Assessment of Business processes	
5	Assessment of requirement of Software requirements	
6	Assess the Integration requirement	
7	Assess the connectivity requirement for field locations (including Building)	
8	Assessment the Network laying requirement	
9	Assessment of training requirement	
Design Phase		
10	Formulation of Solution Architecture	1. Final Bill of Quantity 2. HLD documents 3. LLD documents 4. Application architecture documents. 5. Technical Architecture documents. 6. Network Architecture documents. 7. ER diagrams and other data modeling documents. 8. Logical and physical database design. 9. Data dictionary and data definitions. 10. GUI design (screen design, navigation, etc.).
11	Creation of Detail Drawing	
12	Detailed Design of Smart City Solutions.	
13	Development of test cases (Unit, System Integration and User Acceptance)	
14	Preparation of final bill of quantity and material	
15	SoP preparation	

S. No.	Key Activities	Deliverables
		11. Test Plans 12. SoPs 13. Change management Plan
16	Helpdesk setup	1. IT and Non IT Infrastructure Installation Report 2. Completion of UAT and closure of observations report 3. Training Completion report 4. Application deployment and configuration report
17	Procurement of Equipment , edge devices, COTS software (if any), Licenses	
18	IT and Non IT Infrastructure Installation	
19	Development, Testing and Production environment setup	
20	Network connectivity (All activities other that bandwidth provisioning)	
21	Software Application customization	
22	Development of Bespoke Solution (if any)	
23	Data Migration	
24	Integration with Third party services/application (if any)	
25	Unit and User Acceptance Testing	
26	Preparation of User Manuals , training curriculum and training materials	
27	Role based training(s) on the Smart City Solutions	
Integration Phase		
28	SoP implementation	1. Integration Testing Report
29	Integration with GIS and Command and Control Centre	
30	Other Integrations	
Go –Live		
31	Go Live	1. Go-Live Report
Operation and Maintenance		
32	Operation and Maintenance of IT, Non IT infrastructure and Applications	1. Detailed plan for monitoring of SLAs and performance of the overall system 2. Fortnightly Progress Report 3. Monthly SLA Monitoring Report and Exception Report 4. Quarterly security Report 5. Issues logging and resolution report
33	SLA and Performance Monitoring	
34	Logging, tracking and resolution of issues.	
35	Application enhancement	
36	Patch Updates	
37	Helpdesk services	

6.6 Risk and Mitigations

S. No	Risk	Mitigation
1	There might be inadequate capacity at various levels to co-ordinate with various agencies and to supervise the project implementation	As per the approach, single implementation agency is responsible for implementing, commissioning and managing the network.
2	Inordinate implementation delays would increase the project cost and severely limit the benefit realization	Strong and professional program management framework should be put in place that would ensure delivery of the project at the right time with right quality
3	Lack of ground level support	Workshops to engage all stakeholders should be initiated to get them on-board with the project for providing the necessary clearance for the civil work etc.
4	Theft of Furniture and other equipment's	Detection, Tracking, Monitoring, Management and Control of all critical and non-critical IT equipment and devices through an asset monitoring tool.

7. Service Level Agreements (SLA)

The purpose of this SLA is to clearly define the levels of service to be provided by System Integrator to LSCL during of the maintenance phase or until this SLA has been amended. The objectives of this SLA are to:

a. Trigger a process that applies LSCL and Contractor management attention to some aspect of performance only when that aspect drops below an agreed upon threshold, or target.

b. Makes explicit the performance related expectations on performance required by LSCL

c. Assist the LSCL to control levels and performance of services provided by contractor

For the purpose of defining SLAs, the solution components of CCC are categorized as below –

Category	Solution Components
Category – I	Command and Control Centre Application, Contact Center Application, IBMS, Cloud Based Applications , Network Bandwidth
Category – II	Video Wall, Desktops, Servers, Edge Equipment (Cameras, Sensors etc.)
Category – III	CCC Building Surveillance

The required SLAs for each category of components is provided below -

7.1 Category – I

Availability quarter (calculated separately for each component)	Deduction as % of the apportioned price of total AMC for the specific component of the CCC solution
> 99.95%	NIL
Less than 99.95%	Deduction of 1% of the apportioned price of the apportioned quarterly AMC for every 0.1% or part there of decrease in availability under 99.9%.

7.2 Category – II

Availability quarter (calculated separately for each component)	Deduction as % of the apportioned price of total AMC for the specific component of the CCC solution
> 99.5%	NIL
Less than 99.5%	Deduction of 1% of the apportioned price of the apportioned quarterly AMC for every 0.1% or part there of decrease in availability under 99.9%.

7.3 Category – III

Please refer SLAs defined in the surveillance system DPR.

7.4 Availability Calculation

While calculating availability following shall be considered:

1. The component shall be considered as available if
   a. All component functions described in the specification are executed at periodicities specified in the specification. without degradation in the response times
   b. Information Storage and Retrieval applications are available
   c. Data exchange with other system is available as per pre-defined data exchange method and format
2. Non-Availability of internal and external systems that are not within the scope of CCC solution components shall not be considered for systems availability calculation.
3. Scheduled downtime shall be considered as the non-available time.
4. The computation of Availability / Non-availability would be rounded up to 2 decimal places at each Contract Co-ordination Site on quarterly basis and any deduction in the maintenance charges thereof would be calculated as stated above on pro-rata basis.
5. Availability would be calculated on per quarter basis.

The formula to be used for availability computation would be as under:

Availability per quarter = THQ- (S1 x 1+S2 x0.4+S3 x 0.1) x 100%
Where:

- **THQ** is total hours in the quarter
- **S1** is the total non-available hours in Severity Level-1
- **S2** is the total non-available hours in Severity Level-2
- **S3** is the total non-available hours in Severity Level -3

7.5 Problem Severity Levels

Category	Definition
Severity 1 – Urgent	Complete system failure, severe system instability, loss or failure of any major subsystem or system component such as to cause a significant adverse impact to system availability, performance, or operational capability

Category	Definition
Severity 2 – Serious	Degradation of services or critical functions such as to negatively impact system operation. Failure of any redundant system component such that the normal redundancy is lost Non-availability of Manpower at control center during working hours
Severity 3 – Minor	Any other system defect, failure, or unexpected operation
Severity 4 – General/Technical Help	Request for information, technical configuration assistance, "how to" guidance, and enhancement requests.

7.6 Breach of SLA

In case the contractor does not meet the service levels for three (3) continuous time-periods as specified in the relevant clause, LSCL will treat it as a case of breach of Service Level Agreement. The following steps will be taken in such a case:-

- LSCL issues a show cause notice to the contractor.
- Contractor should reply to the notice within three working days.

Exclusions

The contractor will be exempted from any delays or slippages on SLA parameters arising out of following reasons:-

a. Delay in execution due to delay (in approval, review etc.) from LSCL's side. Any such delays will be notified in written to the IT Team.

b. The network links will be provided by a third party and the contractor will monitor and report any problems on behalf of third party. If contractor notifies and LSCL approves that the delay or fault was due to the third party link services then such loss will not be considered for tracking contractor's SLA parameters.

8. Training and Change Management

Capacity Building is a highly critical component of Command and Control Centre (CCC). The objective of Capacity Building (CB) initiatives is to empower the direct users and other stakeholders of Ludhiana Smart City Limited (LSCL) is to optimally use the system and enhance the outcomes in policing, traffic law enforcement and other core police functions; and also ensure a smooth functioning.

Success of the project, both in short term as well as long term has unswerving dependency on the officials trained on CCC tools and applications. Drawing upon the diverse challenges expected for the implementation of the project, specifically the workforce challenges, it is apparent that capacity building is the need of the hour to further ensure that the project is a success.

The implementation of the CCC and new process will significantly impact the functioning of LSCL in Ludhiana. The challenge will be to empower and support the workforce to understand, learn, and adopt the new ways of working in order to fully realize the potential benefits of this fundamental change.

To manage a large scale implementation, which impacts a large number of users directly or indirectly, a comprehensive and well-structured Capacity Building approach is required. Capacity Building approach would include availability of requisite infrastructure and resources to support the entire program. It would also ensure that the required user groups receive sufficient training to equip them with the skills required to efficiently use or be aware of the new processes and/or systems.

Hence, the objectives of developing a Capacity Building Program are as follows:

- Identify the training audience groups
- Identify Training delivery methods
- Training development and delivery resource
- To motivate, train and capacitate department and police workforce
- To efficiently embark on the revised roles and responsibilities
- Embed sustainability of the project

8.1 Overview of capacity building scope

The SI will have the prime responsibility for executing an end to end capacity building program on behalf of LSCL to meet the desired capacity building objectives. The LSCL will enable the SI to execute the program by providing requisite infrastructural support like providing access for conducting the training, assist in selection of user group and ensuring attendance of the trainees. However, the SI shall be responsible for the following activities under the scope of capacity building plan.

8.2 Identification of Trainers

The scope of the capacity building envisages identification of qualified trainers with equipment experience and training competency within the department. SI would be responsible for training the selected trainers and building their capacity for ICCC. These trainers will be responsible for implementing the Capacity Building interventions beyond the scope of the System Integrator.

8.3 Develop Overall Training Plan

The SI shall be responsible for finalizing a detailed training plan for the program in consultation with LSCL covering the training strategy, environment, training need analysis and role based training curriculum with timelines. SI shall own the overall training plan working closely with the LSCL team.

8.4 Develop Training schedule and curriculum

The SI shall develop and manage the training schedule in consultation with LSCL, aligned with the overall implementation roadmap of the project and coordinate the same with all parties involved. Training schedule shall be developed and optimized in order to reduce business impact and enable effective utilization of Training infrastructure and capacities.

The training curriculum for the training program should be organized by modules and these should be used to develop the training materials. The training curriculum shall outline the mode of delivery, module structure duration and target audience.

Training sessions should be conducted such that identified trainees of the application/modules are trained by the time the application reaches “go-live” with possibly no more than a week’s gap between completion of training and going live of application. Continuous reporting (MIS) and assessment should be an integral function of training. SI shall also identify the languages to be used by the end-user for entering data and ensuring multi-language (English & regional) training to the end users as per requirement.

8.5 Develop Training Themes and Material

Based on their needs and the objectives of the Command and Control Centre project, training programs could be organized under the following themes:

1. Basic IT skills and use of computers to create awareness about the benefits of ICT and basic computer skills.

2. Role-based training on the Command and Control application – Basic and Advanced. This training should be in a role based, benchmarked and standardized format, multi-lingual and lead to learning and assessment. It should also allow for self-learning and retraining. Training should include mechanism for demonstration using audio/video/simulated demo/ practice exercises etc.

3. “Train the Trainer” programs, where members of the departments would be trained to enable them to conduct further training programs, thus helping to build up scalability in the training program and also reducing the dependency on external vendors for training.

4. System Administrator training: a few members of the department with high aptitude would be trained to act as system administrators and trouble-shooters for tools and applications.

5. Customization of the Training Manuals, User Manuals, Operational and Maintenance Manuals provided along with the Command and Control Centre applications.

6. Design and development of the Training Manuals, User Manuals, Operational and Maintenance Manuals for the modules developed.

In cases where the training material will be made available by LSCL, it is the SI's responsibility to ensure the relevance of the material, customize if necessary and own up the delivery and effectiveness.

SI shall ensure that the training content meets all the objectives of the training course. SI shall also develop the training material for Computer Based Training, Instructor Led Training, Online User Material/Help Manuals and Job Aids.

SI shall provide detailed training material providing step-by-step approach in soft and hard copies to all concerned officials for reference.

8.6 Deliver Training to End Users

SI shall deliver training to the end users utilizing the infrastructure of the LSCL. Role-based training for the Senior Officers will be carried out by the System Integrator at the location identified by LSCL.

SI shall also impart simulated training with some real life city command and control center scenarios. The SI should create case studies and simulation modules that would be as close to the real life scenario as possible. The objective of conducting such trainings would be to give first-hand view of benefits of Command and Control Centre.

This training needs to be conducted by the SI at the very end when all the other trainings are successfully completed. This training may seem similar to role based training mentioned in the section above. However, in this simulated training, the SI would ensure that the relevant officials are provided an environment that would be exactly similar to the one at the CCC.

Most of the trainings would be an Instructor-Led Training (ILT) conducted by trained and qualified instructors in a classroom setting. To maintain consistency across command and control centre system trainings, standard templates should be used for each component of a module.

An ILT course will have the following components:

- Course Presentation (PowerPoint)
- Instructor Demonstrations (Application training environment)
- Hands-on Exercises (Application training environment)

- Application Simulations: Miniature version of command and control centre application with dummy scenarios providing exposure to concerned officials to a real life scenario post implementation of command and control centre project

- Job Aids (if required)

- Course Evaluations (Inquisition)

In addition to the ILT, for the modules that may be more appropriate to be conducted through a Computer Based Training (CBT), CBT should be developed for them. CBT should involve training delivered through computers with self-instructions, screenshots and simulated process walk-through and self-assessment modules.

Selected set of LSCL with high aptitude group and/or relevant prior training, are to be imparted with the training/skills to act as system administrators and also as trouble-shooters with basic systems maintenance tasks including hardware and network.

8.7 Deliver Training to Trainers

SI shall coordinate the 'Train the Trainer' session for the identified trainers to ensure that they have the capability to deliver efficient training. In addition to the end-user training sessions, Training to Trainers will consist of following three segments:

1. The first segment will be set of workshops covering effective presentation skills and coaching techniques and discussing the benefits and structure of the trainer model.

2. The second segment will be the formal command and control centre system training which will consist of all modules of command and control system relevant for various roles in LSCL.

3. The third segment will be a teach-back session where trained trainers will present course content and receive feedback regarding content, flow, and presentation techniques. This will also include a feedback session where trainers can provide feedback on the training materials, flow, comprehension level, and accuracy.

8.8 Training effectiveness evaluation

SI shall evaluate the effectiveness of all end users trainings using electronic or manual surveys. SI shall be responsible for analyzing the feedback and arrange for conducting refresher training, wherever needed. SI will also be bound by the capacity building SLA.

LSCL will periodically monitor the training effectiveness through the performance metrics and Service levels and the SI shall comply with the same.

8.9 Implementation Plan

Training and Capacity Building Plan

Capacity Building for CCC Project will allow LSCL to manage day to day challenges faced as a result of the project and to ensure a sustainable operating model during and after implementation and stabilization.

Building capacities at various levels is critical to the successful implementation of the recommended command and control center initiative. Also, the training programs would cover general/basic computer awareness programs in addition to command and control center system-specific programs to ensure adoption of the system.

This section covers a broad training and capacity building plan to be followed by the SI. However, the SI is required to validate the same and make amendments as per the solution offered. The training plan will have to be shared with LSCL and approved prior to being executed by the SI.

Main Training Themes

Based on the needs and the objectives of command and control center project, training programs would be organized under the following themes:

1. Creating awareness about the benefits of ICT and basic computer skills
2. Role-based training on the command and control centre applications
3. "Train the Trainer" programs, where members of the LSCL staff would be trained to enable them to conduct further training programs, thus helping build up scalability in the training program and also reducing the dependency on external vendors for training.
4. System Administrator training: a few members of the LSCL staff with high aptitude would be trained to act as system administrators and trouble-shooters for command and control centre system.

The above themes are expanded as below:

1. **Creating awareness and sensitization regarding the benefits of ICT; and creating Basic Computer Skills**
   - This part of the training focuses on the awareness of the general benefits of IT systems such as automation of routine and redundant tasks or moving from the paper-based records management to a more sophisticated electronic records system that can alleviate the efforts to create reports for senior management.
   - Fundamentals of computer usage should focus on the basics of using the computer, keyboard, and mouse in order to make the users feel comfortable with the computer.
   - Email and Office suite training
   - Training on analytical functions of the computers such as worksheet applications should be imparted to the users to actually derive the benefits of analysing the data.

2. **Role based training on application software**

- The training should focus on the police officials getting comfortable to command and control canter system workflow as per their role and build skills to use CCC applications in day to day operations.
- This training would be tailored according to the unique requirements of each user category. The training program must ensure to cover the following user categories:

Hierarchy	Rank
Senior Management	• IAS Officers, PCS Officers
Middle Management	• Chief Executives
Lower Management	• Departmental Officers

3. **"Train the Trainer" Programs**

- Selected set of LSCL staff with high aptitude group and/or relevant prior training, are to be trained as trainers who would, in turn, train their colleagues.
- "Train the Trainer" program could be held at a central location
- The trained trainers would, in turn, conduct training programs for their colleagues
- Trainers would be trained to impart training in basic computer awareness & skills, and role-based training on command and control centre system.

4. **Specialized training on system administration and troubleshooting:**

Select set of LSCL staff with high aptitude group and/or relevant prior training, are to be imparted with the training/skills to act as system administrators and also as trouble-shooters with basic systems maintenance tasks including hardware and network.

8.10 Indicative Training Plan for the Members of LSCL Department

The following is an indicative training plan for members based on the nature of their responsibilities:

S. No.	Name of the Training Programme	Frequency	Indicative Duration (Days)	Average Batch Size
1	Orientation to change management	Once	3	10
2	Change Management	Once	2	10
3	CCC Application, DC, functioning and back office operations	Twice	2	5

S. No.	Name of the Training Programme	Frequency	Indicative Duration (Days)	Average Batch Size
4	Teamwork Skills	Once	2	20
5	Project Management	Once	5	5
6	Orientation to IT & Computers	Twice	2	20
7	Orientation to Command and Control Centre applications & its benefits	Twice	2	5
8	Information Security & IT Infrastructure Security	Once	1	5
9	Data Center & Network Administration	Once	2	5
10	Hardware component Installation & Maintenance	Once	2	5
11	Management Information System / Reporting	Twice	2	5

9. Assumptions

The following are the assumptions considered while preparation of this DPR:

1. LSCL will provide representatives from other City agencies namely – police, traffic, electricity, water and sewerage for effective monitoring of city coordination for resolution of reported incidents.

2. The resolution of incidents shall be the responsibility of the respective agency to which the incident has been assigned for resolution.

3. The System integrator will not be responsible for creation of any physical infrastructure to the Integrated Command and Control Centre.

   - Design, Procurement, Construction, Testing and Commissioning of -

     a. CCC Facility Physical Build

     b. Electrical and Mechanical Components

     c. Electrical Distribution Room

4. Appropriate Data Center space and facilities required for installation of required hardware and systems thereon shall be provided as part of common infrastructure setup.

5. All services that needs to be integrated should be ready for integration before the commissioning of Integrated Command and Control Centre:

6. Open API's shall be made available or to be developed by respective vendor for the respective systems which needs to be integrated. Furthermore, in cases, wherein, API's are not available then respective user licenses shall be made available by LSCL.

7. The Cost of the consumables such as such as printer cartridges, papers, diesel for Genset, Paper Cups and other should be borne by the SI maintain regular operations.

8. The Data Centre shall be In-house and collocated with the ICCC

9. Disaster Recovery on Public Cloud

10. Cost of Operational Manpower shall be borne by LSCL

11. Electricity Charges for consumption at ICCC to be borne by LSCL

12. GIS Maps with relevant layers to be made available by LSCL

13. Bandwidth from ICCC to Cloud DC, DR and other Systems to be borne by MSI. design

10. Technical Specifications

10.1 Schedule – I (Video Wall)

Video Wall Screen

The Video Wall for CCC shall be configured with 4x4 formation of the following Professional Display (LED Display Cube) Screens:

S. No.	Parameter	Minimum Specifications
1	Technology	DLP LED Suitable for Video Wall Display
2	Screen Size	50”
3	Panel Technology	Vertical Alignment (VA)
4	Native Resolution	1920 x 1080 (Full HD) Pixels
5	Aspect Ratio	16:9
6	Pixel Pitch	0.53025 (H) X 0.53025 (W)
7	Static Contrast Ratio (Minimum)	1800:1 or better
8	Dynamic Contrast Ratio (Minimum)	1000000:1 or more
9	Brightness	700 (or above) nit
10	Brightness of projection engines	Minimum 2000 lumens
11	Brightness uniformity	>= 98%
12	Viewing angle	178 degree/178 degree (H/V)
13	Response time	8ms
14	Bezel Width	3.4 mm or less
15	Screen to Screen Gap	<= 1 mm
16	Input	HDMI,VGA, Digital DVI, Display Port, HDBase T & other inputs as per Video Wall solution offered
17	Operations	365 X 7 X 24
18	Accessories	All Included (AC Power Cord, Remote Control, Adjustable Wall Mount Bracket, Necessary Cables And Connectors etc.)
19	Monitoring of critical parameters to ensure stable operation of the system 24 x 7	Internal temperature, Ambient temperature, humidity, Brightness, Cooling, Light source status
20	Cube control & monitoring	Video wall should be equipped with a cube control & monitoring system, Should be able to control & monitor individual cube , multiple cubes and multiple video walls, Provide video wall status including Source ,

S. No.	Parameter	Minimum Specifications
		light source ,temperature, fan and power information, Should provide a virtual remote on the screen to control the video wall, System should have a quick monitor area to access critical functions of the video wall
21	Dust prevention	Should meet or exceed IP6X standard. Certificate to this effect to be furnished from 3rd party Laboratory
22	Control	IP based control to be provided
23	Remote	IR remote control should also be provided for quick access
24	Light Source Type	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.

Video Wall Controller

S.N.	Parameters	Minimum Requirements
1	Controller	Controller to control Video wall in a matrix form as per requirement
2	Chassis	19" Rack mount
3	Processor	Latest Generation 64 bit x86 Quad Core processor (3.4 Ghz) or better
4	Operating System	Pre-loaded latest 64-bit Operating System Windows / Linux / Equivalent, with recovery disc
5	RAM	16 GB DDR3 RAM or higher
6	HDD	500 GB or higher Solid State Disk
7	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports
8	RAID	Should support all RAID levels
9	Power Supply	(1+1) Redundant hot swappable
10	Input/ Output support	DVI/HDMI/USB/ LAN/ VGA/SATA port
11	Accessories	104 key Keyboard and Optical USB mouse
12	USB Ports	Minimum 4 USB Ports
13	Redundancy support	Power Supply, HDD, LAN port & Controller
14	Scalability	Display multiple source windows in any size, anywhere on the wall
15	Control functions	Brightness/ Contrast/ Saturation/ Hue/Filtering/ Crop/ Rotate
16	Inputs	To connect to minimum 2 sources through HDMI
17	Output	To connect Displays through HDMI/DVI as per requirements
18	Operating Temperature	10°C to 35°C, 80 % humidity
19	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units

Video Wall Management Software

S. No.	Parameter	Minimum Specifications
1	Display & Scaling	Display multiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
3	Scenarios management	Save and Load desktop layouts from Local or remote machines
4	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop Application
5	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop
6	Other features	SMTP support Remote Control over LAN Alarm management Remote management Multiple concurrent client KVM support
7	Cube Management	Cube Health Monitoring Pop-Up Alert Service Graphical User Interface
8	General requirement	The wall management software shall be having interoperability with Video management system The wall management software may be centrally Server based or local controller based architecture
9	General Requirement	Key features of Wall management Software a. Central configuration database b. The Wall Control software shall perform health monitoring that allows timely detection of faults. i. Wall health ii. Cube health iii. Cube IP-address iv. Brightness c. Shall allow commands on the wall level or cube level or a selection of cubes i. Switching entire display wall on or off ii. Fine tune colour of each cube d. Log file function
10	General Requirement	a) The software should be able to pre-configure various display layouts and access them at any time with simple mouse click or based upon timer b) The software should enable users to see desktop of graphics display wall remotely on any PC connected with the Display Controller over the Ethernet and change the size and position of various windows being shown.

S. No.	Parameter	Minimum Specifications
		c) Wall management software shall be having interoperability with Video Management System d) The video wall management software may be centrally server based or local controller based architecture. e) The software should enable various operators to access the display wall from local keyboard and mouse of their workstation connected with the display controller on the Ethernet. f) 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 movable windows in real time environment. g)

Audio Mixer & Speaker System

S. No.	Parameter	Minimum Specifications
1.	Audio Mixer	Input Power 6W RMS
2.	Frequency Response (-3dB)	80Hz - 20kHz
3.	Frequency Range (-10dB)	74Hz - 54kHz
4.	System Sensitivity (1W @1m)	89dB (1W = 4V for 16 Ohms)
5.	Nominal Impedance	16 Ohms
6.	Speaker Mounting	Ceiling Speaker
7.	SNR	>= 70 dB
8.	Speaker Out	100 V AB 6 Zone Speaker Output
9.	Rated Power Out	240W
10.	Fireman Microphone	500 Mv, 600Ω
11.	Line 1-2 inputs	385mV, 10kΩ balanced Combo
12.	Line 3-6 inputs	350mV, 10kΩ, RCA
13.	Operation Environment	Operation Temp: +5 °C ~ +40 °C Store Temp:-20 °C ~ +70 °C Operation Humidity: <95%
14.	Power Consumption	600

10.2 Schedule – II (CCC Core Applications)

Details Covered in Functional Specifications under Section 4.

10.3 Schedule – III (CCC Hardware)

Network Colour Multi-Function Laser Printer

#	Parameter	Minimum Specifications
1.	Print Speed	Black : 16 ppm or above on A3, 24 ppm or above on A4 Color : 8 ppm or above on A3, 12 ppm or above on A4
2.	Copy Speed	12 ppm or better
3.	Scanner	Flatbed type with ADF
4.	Resolution	600 X 1200 DPI
5.	Memory	1 GB or more
6.	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes
7.	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray
8.	Duty Cycle	25,000 sheets or better per month
9.	OS Support	Latest version of Linux, Windows 10, 7, 8, 8.1
10.	Interface	Fast Ethernet (100Base-T),Hi-Speed USB 2.0 , Wi-Fi
11.	General	Full toner Cartridge shall be supplied with the printer
12.	General	Printer shall be accompanied with necessary accessories such as driver media, connecting cables, power cables, etc.

Work Station for City Management Room with Joy Stick and Dual Monitor

#	Parameter	Minimum Specifications
1.	Processor	Latest Quad Core i7 with 3 GHz or higher
2.	Chipset	Compatible 64 bit Chipset
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
7.	Media Drive	No CD / DVD Drive

#	Parameter	Minimum Specifications
8.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10.	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)
11.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard
12.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms
13.	PTZ joystick controller (with 2 of the workstations in SCOC)	• PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered • Hall-effect joystick with three axis i.e. X/Y: for pan and tilt; Z: knob for zoom and 6 application defined hotkeys • Jog Dial : 6 application defined hotkeys • Vector solving with twisting & return to center head • Operating cycle > 50,00,000 cycles or better • Deflection : Pan/Tilt (XY): ±15° and Zoom (Z): ±25°
14.	Monitor	Two monitors of 22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time
15.	Certification	Energy star /BEE certified/EPEAT
16.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.
17.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
18.	Power Input	100 -240V AC
19.	Graphic Card	Extra graphics card for support visuals

Manager Work Station with Touch Screen Monitor

#	Parameter	Minimum Specifications
1.	Processor	Latest Quad Core i7 with 3 GHz or higher

#	Parameter	Minimum Specifications
2.	Chipset	Compatible 64 bit Chipset
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD. Provision for installing 4 more drives.
7.	Media Drive	NO CD / DVD Drive
8.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9.	Audio	Line/Mic IN, Line-out/Spr Out (3.5 mm)
10.	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)
11.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard
12.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms
13.	Monitor	Touchscreen monitor with 27 Inches screen , Wide LED, Resolution- 1920x1080, Aspect Ratio-16:9 , refresh rate 5ms or better
14.	Certification	Energy star /BEE certified/EPEAT
15.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.
16.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
17.	Power Input	100 -240V AC

Help Desk Team/ Contact Centre/ War Room/ Security/ Technical Support Team Work Stations

#	Parameter	Minimum Specifications
1.	Processor	Latest Quad Core i7 with 3 GHz or higher
2.	Chipset	Compatible 64 bit Chipset
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 or higher expandable up to 32 GB or more
5.	Graphics card	Minimum Graphics card with 2 GB video memory (non- shared)
6.	HDD	2 TB SATA-3 Hard drive @7200 rpm with Flash Cache of 64GB SSD.

#	Parameter	Minimum Specifications
		Provision for installing 4 more drives.
7.	Media Drive	NO CD / DVD Drive
8.	Network interface	10/100/1000 Mbps autosensing on board integrated RJ-45 Ethernet port.
9.	Audio	Line/Mic IN, Line-out/Speaker Out (3.5 mm)
10.	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)
11.	Keyboard	107 or more English + Punjabi and Rupee symbol Keys keyboard
12.	Mouse	2 Or 3 button USB Optical Scroll Mouse with antistatic mouse pad resolution of Optical 1000 CPI, Complying to CE and FCC norms
13.	Monitor	22” TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time
14.	Certification	Energy star /BEE certified/ EPEAT
15.	Operating System	Pre-Loaded Windows 10 with recovery disc, Linux etc.
16.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
17.	Power Input	100 -240V AC

IP Phone

#	Parameter	Minimum Specifications
1	Display	2 line or more, Monochrome display for viewing features like messages, directory
2	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface
3	Speaker Phone	Yes
4	Headset	Wired, Cushion Padded Dual Ear-Speaker, Noise Cancelling headset with mouthpiece microphone, port compatibility with IP Phone
5	VoIP Protocol	SIP V2
6	POE	IEEE 802.3af or better
7	Supported Protocols	SNMP, DHCP, DNS
8	Codecs	G.711, G.722, G.729 including handset and speakerphone

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

Digital Set Top Box

#	Standards
1	The equipment must confirm to standards and specifications laid down by Government of India.
2	Refer a) Digital Set Top Box for Direct-To-Home (DTH) Services Specifications issued by Bureau of Indian Standards, Govt. of India b) Consultation Paper on Technical Interoperability of DTH Set Top Boxes issued by Telecom Regulatory Authority of India (TRAI), Govt. of India

Television Set for Meeting room

#	Parameter	Minimum Specifications
1	Technology	LED Backlit Full HD TV
2	Screen Size	55" or higher
3	Native Resolution	Full HD(1920 x 1080 progressive signal)
4	Aspect Ratio	16:9
5	Static Contrast Ratio (Minimum)	4500:1 or better
6	Dynamic Contrast Ratio (Minimum)	Up to 50000
7	Brightness	350 nit or better
8	Response time	8ms
9	Input	2 HDMI , 1 DVI and USB
10	Output Port	Audio

10.4 Schedule – IV (ICCC Civil & Infrastructure)

Civil Work (False Floor, Ceiling, Ducting, Access Doors, Painting, Partitioning etc) covered under Section 4.

10.5 Schedule – V (Contact Centre Application)

#	Parameters
1	For up to 50 agents
2	Automatic call distribution
3	Automatic identification of incoming number based on landline and mobile number mapping
4	Call recording mapped to incident tickets
5	Customizable agent and supervisor desktop layout
6	Inbound and outbound capability
7	Call control
8	Multisession web chat
9	Email
10	Live data reporting gadgets
11	Phonebook
12	Multiline support
13	Speed dial in IP phones

Automatic Call Distribution (ACD)

1) Should be highly available with hot standby and seamless failover in case of main server failure. There should not be any downtime of Contact Center in case of single server failure.
2) Should support skill based routing and it should be possible to put all the agents in to a single skill group and different skill groups
3) ACD support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialled number etc.
4) ACD should support call routing based on longest available agent, circular agent selection algorithms.
5) 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.
6) Agents should be able to chat with other Agents or supervisor from the Agent desktop software
7) Supervisor should be able to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop
8) Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.
9) 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.

Interactive Voice Response (IVR)

1) IVR should play welcome messages to callers Prompts to press and collect DTMF digits
2) IVR should be able to integrate with backend database for self-service, as and when required.
3) GUI based tool to be provided for designing the IVR and ACD call flow.
4) IVR should support VoiceXML for ASR, TTS, and DTMF call flows
5) IVR should be able to Read data from HTTP and XML Pages
6) IVR should be able to run outbound campaigns.
7) IVR should be able to record calls.

Reporting

1) System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic analysis reports etc
2) Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes
3) Queue reports, Abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.
4) Reporting platform to support custom reports using a combination of the Crystal Reports Developer's Toolkit and SQL stored procedures.
5) Users of the Historical Reports should be able to perform the following functions View, print, and save reports. Sort and filter reports, Send scheduled reports to a file or to a printer. Export reports in a variety of formats, including PDF, RTF, XML, and CSV.

E-mail

6) Administrator should be able to assign one or more email addresses to a single Queue.
7) Email routing support integration with Microsoft Exchange 2003 or Microsoft Exchange 2007 or 2010.
8) Agents should be able to automatically resume of e-mail processing on voice disconnect.
9) Agent should be able to save email draft response and resume at a later time.
10) Agent should be able to re-queue email.
11) Supervisor should be able to access real-time reporting for Agent E-Mail mail volume by Queue

10.6 Schedule – VI (WAR Room /Situational Room)

LED display to present critical information Display

#	Parameter	Minimum Specifications
1	Technology	LED Backlit Full HD TV
2	Screen Size	55" or higher
3	Native Resolution	Full HD(1920 x 1080 progressive signal)
4	Aspect Ratio	16:9
5	Static Contrast Ratio (Minimum)	4500:1 or better
6	Dynamic Contrast Ratio (Minimum)	Up to 50000
7	Brightness	350 nit or better
8	Response time	8ms
9	Input	2 HDMI , 1 DVI and USB
10	Output Port	Audio

Over Head Projector

#	Parameter	Minimum Specifications
1	Display Technology	Poly-silicon TFT 3LCD
2	Resolution	WXGA, 1280x800, 16:10
3	Colours	1.07 billion Colours
4	Brightness	4000 or more ANSI lumens (in Normal Mode)
5	Contrast Ratio	2200:1 / 10000:1 (dynamic)
6	Video Input	One computer (D-Sub, Standard 15 pin VGA connector) One HDMI
7	Keystone Correction	Horizontal and vertical
8	Zoom and Focus	Manual Zoom and Focus
9	Audio	Internal speaker
10	Remote Operations	Full function Infrared Remote Control
11	Other features	Auto source detect, Auto-Synchronization, Keystone Correction
12	Mounting	Ceiling mount with fixed structure, with all accessories and cables
13	Lamp Life	Up to 3000 hour(s) / up to 5000 hour(s) (economic mode)
14	Lamp Type	260 Watt
15	Lens aperture	F/2.4-2.66
16	Power	AC 230 V (50 Hz) Projection Distance: 4 ft. - 33 ft.
17	General	a) 3D Capable – Yes b) Device Type: Projector with High Definition 720p

#	Parameter	Minimum Specifications
		or better display c) Min. Operating Temp : 2°C d) Max. Operating Temp: 48°C e) Security Lockup Slot – Yes f) Sound Emission : 37dB g) Sound Emission (Economic mode): 32dB h) Integrated speakers - Yes i) Throw Ratio : 1.28 – 1.536 :1 j) Video Inputs: RGB, Component Video (PAL – B/G, PAL-N, PAL-M, PAL-I, NTSE 4.43, NTSE 3.58, PAL-D, SECAM-L, PAL-H, SECAM-K1, SECAM-D/K, SECAM-B/G) k) Video Interfaces : HDMI & VGA l) Video Modes: 480p, 720p, 1080p, 480i, 576i, 576p m) Zoom Factor – Min. 1.2x

10.7 Schedule – VII (IP PABX system)

IP PABX System

- ✓ The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture
- ✓ 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
- ✓ The system should be based on server gateway architecture with external server running on Linux OS. No card based processor systems should be quoted
- ✓ The voice network architecture and call control functionality should be based on SIP
- ✓ The call control system should be fully redundant solution with no single point of failure & should provide 1:1 redundancy.
- ✓ The communication server and gateway should support IP V6 from day one so as to be future proof
- ✓ The entire solution (IP PBX, its hardware, IP Phones, Voice Gateway) should be from a single OEM

Support for call-processing and call-control

- ✓ Should support signalling standards/Protocols – SIP, MGCP, H.323, Q.Sig
- ✓ Voice Codec support - G.711, G.729, G.729ab, g.722, ILBC
- ✓ The System should have GUI support web based management console

Security

- ✓ The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS

- ✓ System should support MLPP feature
- ✓ Proposed system should support SRTP for media encryption and signalling encryption by TLS
- ✓ 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
- ✓ The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server
- ✓ Voice gateway to be provided with 1 PRI card scalable to 3 PRI in future for PSTN (PRI) line termination.

PRI Modem Pair

S.N.	Module	Parameter	Minimum Specifications
1	Power Device	Voltage Required	AC 110/220 V
		Voltage Required Margin	± 10%
		Frequency Required	50/60 Hz
		Power Consumption Operational	200 Watt
		Type	Internal power supply
2	Modem	Type	ISDN terminal adapter
		Enclosure Type	integrated
		Max Transfer Rate	1.5 Mbps
		Digital Ports Quantity	30
		Digital Signaling Protocol	ISDN PRI
3	Networking	Type	remote access server
		Connectivity Technology	wired
		Data Link Protocol	EtherTalk, Ethernet, HDLC, ISDN
		Network / Transport Protocol	AppleTalk, IPX/SPX, TCP/IP
		Features	CHAP authentication, PAP authentication, firewall protection
		Compliant Standards	IEEE 802.3
		Switching Protocol	Ethernet, Frame Relay, PPP
		Remote Management Protocol	SNMP
		Line Rate	E-1
		Framing Format	D4, G.703
4	Communication	Digital Signaling Protocol	ISDN PRI
		Protocols & Specifications	V.110 (I.470), V.120 (I.464)
		Digital Ports Quantity	30
		Digital Ports Quantity	30
5	Interface	Gender	female
		Connector Quantity	1, 30
		Type	modem, serial
		Interface	ISDN PRI E1, V.35

S.N.	Module	Parameter	Minimum Specifications
		Quantity	1, 30
		Connector Type	44 pin D-Sub (DB-44), RJ-48
6	Environmental Parameters	Min Operating Temperature	32 °F
		Max Operating Temperature	104 °F
		Humidity Range Operating	5 - 90%

SMS Gateway

- ✓ Bidder has to provide SMS Gateway of Telecom Service Provider which has ability to withstand for continued growth in A2P SMS and SVI SMSG.
- ✓ The SMS Gateway PULL SMS application must have security features to ensure confidentiality of sensitive customer data.
- ✓ The SMS Gateway PULL SMS application should be able to retrieve SMSs sent to one or more short codes / virtual numbers.
- ✓ The SMS Gateway PUSH SMS application should be able to send messages at different priority levels.
- ✓ The SMS Gateway PUSH SMS application must have ability to set working hours and days.
- ✓ The solution should offer configurable mechanism in terms of number of retries and time duration for each retry for messages that could not be sent / delivered immediately.
- ✓ Online mechanism in real time mode has to be provided for SLA enforcement with regard uptime of Push / Pull services & deliveries along with the flexibility to generate MIS on daily / weekly / fortnightly / monthly / between specified data range.
- ✓ Check should be properly imposed to avoid duplicate or multiple SMS delivery to stakeholders.

10.8 Schedule – VIII (Furniture)

Operator Console Table & Ergonomic Chair

#	Parameter	Minimum Specification
1.	Physical Structure	Ergonomically designed desk to ensure 24x7 desking solution with sufficient knee space (min 450mm) and foot space (min 600 mm) and minimum width of 1800 mm.
2.	Working Surface material	The Console Top / working surface should be made of minimum 25 mm thick MDF with High Pressure Laminate finish. The laminate shall be fire retardant, Insulated, Water Proof, Scratch resistant and high hardness. The Table Top should be able to mount three 27 Inches Display monitors for each work station with front edge of the table top should be molded polyurethane edge(for wrist cushion)
3.	Console Design	Consoles must be of modular design, facilitating future equipment retrofits and full reconfigurations without requiring any major modification to the structure or exterior elements

#	Parameter	Minimum Specification
4.	Equipment Mounting	The workstation shall be able to house computer equipment's, Ethernet Points, Power Distribution Unit. The CPUs shall be mounted on Slide out CPU trays (mounted on Heavy duty slides) for ease in maintenance, all of these equipment's should be concealed from direct human view
5.	Frame material	Made of heavy duty Aluminium. The Extrusions shall be duly powder coated with 40+ micron over all surfaces.
6.	Monitor Arms and Rear Walls	Die cast mounted Aluminium articulated arm; fixed firmly on MS Pole with powder coating mounted on its rear wall also made of aluminium Monitor and Functional holder shall guarantee optimum viewing distance. All ergonomic aspects shall be taken in to account. It shall be capable for mounting all type of LCD/LED display with Dimensions between 17” to 27” using suitable brackets/additional base plate For configuration of working position, it shall allow the technical staff to rotate/ tilt/ raise/the monitors as well as fix their adjustment in a quick and easy manner
7.	Warranty/Guarantee	10 years replaceable
8.	Certifications / compliant	ISO 11064 latest revision, BIFMA X5.5, RoHS (UL certificate), Seismic zone IV compliant
Chairs		
1.	General	Ergonomic Chair with Arm Rest and castor wheels designed for 24/7 usage
2.	Backrest support	Tilt adjustable, polystyrene support frame with 100% polyester fiber
3.	Seat Support	Height adjustable, Molded wood, 10 mm. thick with polyurethane foam, density minimum 70 kg/m3
4.	Seat Adjustment Mechanism	Self-adjustable synchronous mechanism with soft resort. Multi-locking with safe anti-return system.
5.	Armrests	Height adjustable via button, Front/back adjustable with PU pads (50 mm)
6.	Column	Class 3 built-in cartridge cylinder steel tube
7.	Base	Swivel on castor with 5 polyamide double-wheel castors (made of polyamide and fiber glass)
8.	Colour	Black
9.	Warranty	Minimum 5 replaceable years
10.	Parameter	Minimum Specification

10.9 Schedule – IX (Building Utilities)

DG Set

#	Parameters	Specifications
1.	Rating (KVA)	250
2.	Rated (KWe)	40
3.	No of Cylinders	4
4.	Rated Speed RPM	1500
5.	Cooling System (Air Cooled/Water Cooled)	Water
6.	Door Type	DD
7.	Side lifting DG set dimensions with top hood, if any (mm)	L x W x H (2770x1150x1800)
8.	Integrated Fuel Tank Capacity (liters)	150
9.	Approximate Dry Weight of DG set (Kg)	1250
10.	Centre lifting DG set dimensions with top hood, if any (mm)	L x W x H (2800x1150x1540)
11.	BHP	84
12.	Power Factor	0.8
13.	Voltage	230 (1Ø) & 415 (3Ø)
14.	Noise Level	<75 dB
15.	Fuel Tank Capacity	65 Ltrs. Or More
16.	Electrical Battery starting voltage	12 V
17.	Lube Oil Change Period	500 Hrs or more
18.	Overload Capacity	10% for one hour in any 12 hours of continuous operations
19.	Redundancy configuration	Should be able to be configured for redundancy from two phases
20.	Control	Automatic Stop device if any parameters are varied beyond upper / lower limits. Integral mounting of instrument panel complete with wiring (for engine) and connections.
21.	Fuel Tank & Piping	Fuel tank to be located within 10 meter periphery of the DG set.
22.	Lubrication	Lube Oil
23.	Heat Exchanger	Yes required
24.	Enclosure	Sound proof, drip proof and Screen protected (min.as per IP 23). The alternator terminal box shall be amended and made suitable for bus duct arrangement.
25.	Alternator	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. It should give rated output at NTP condition. Alternator

#	Parameters	Specifications
		shall have space neater which shall be connected with breaker NO/NC contacts and this should be able to cut off with thermostat. Alternator shall have RTD and BTD.
26.	Acoustics	Acoustic treatment shall ensure a maximum sound pressure not more than 68 dB at 1 meter during the day and 45 dB at neighbor's premises during night while running on partial or full load. The condition shall apply to the engine exhaust noise levels also. A vertical type "Critical" silencer shall be fitted on the exhaust pine.
27.	Insulation Class	Class H
28.	Bearings	Heavy duty pre-lubricated
29.	Ventilation	Centrifugal Fan
30.	Space Heater	Yes to be provided
31.	Total losses as % of rated KW	Not more than 4

IBMS

The MSI shall supply, install and commission BAS, Access control and Physical security system for ICCC Building Office. MSI has to also provide all necessary hardware and all operating and applications software necessary to perform the control sequences of operation as called for in this specification. All components of the system –, application controllers, unitary controllers, etc. shall communicate using the BACnet protocol, as defined by ASHRAE Standard 135-2007, or EIA standard 709.1, the LonTalk™ protocol, or Modbus protocol. At a minimum, provide controls for the following:

1. Air handling units
2. Return air fans
3. Exhaust and supply fans
4. Chilled water system including pumps, chillers, and cooling towers
5. Boilers including hot water pumps
6. Computer room air handling units
7. Refrigerant leak detection system
8. Smoke evacuation sequence of AHUs and return fans including smoke control dampers and fire command override panel.
9. Finned tube radiation control
10. Variable volume and constant volume box control including interlocks with finned tube radiation.
11. Cabinet unit heater controls
12. Monitoring points for packaged equipment such as emergency generators,
13. Power wiring to DDC devices, smoke control dampers and BAS panels except as otherwise specified.

Access Control System

- The Access Controller's should be designed for both critical government & private sector security applications. Below input & output modules should be on-board with the Controllers.
  - Universal Inputs : 12
  - Reader Inputs : 8
  - Tamper Input : 1
  - Digital Lock Output : 4
- The Access Controller's should be designed to support both entry & egress readers while supplying +5 or +12 VDC to each reader.
- The controller should support the data transfer rates up to 100 Mbps and should have IPSec/IKE encryption and authentication. Encryption (up to 192-bit) and authentication may be enabled for communication to and from workstations and controllers. Controller should utilize Internet Protocol Security (IPSec) and Internet Key Exchange (IKE) for its encryption to assure tamperproof communications over the Ethernet.
- The Controller should be perfect for large systems. A controller servicing up to 8 areas can hold 480,000 personnel records. With such a large local storage capacity, access decisions can be made swiftly without waiting for validation by a remote server.
- Controller should have inbuilt 32 MB of flash memory and 128 MB of DDR SDRAM. The flash memory is used to preserve 12 MB of application and run-time data. The dynamic RAM is partitioned for dedicated functions: a full 12 MB for applications, 48 MB for personnel records and 8 MB for the operating system. The unused memory should be available for future enhancements. Personnel record data should be preserved using on-board batteries that can hold the data for at least 7 days without the use of an external UPS. If the controller has its application stored in flash and power loss lasts longer than what the battery can supply for RAM, the controller will send a message to Cyber Station and request that the personnel records automatically be reloaded when the power returns.
- The reader inputs should be powered by a dedicated processor allowing the controllers to support current and future devices for advanced applications. The hardware should be ready to support 260-bit encrypted data messages from the reader.
- It is important for controller to be able to contain potential threats when they are detected. The Controller should respond to Area Lockdown commands set from Access control software providing a quick method of sealing off areas. A simple click of a graphic or an automatic program response is all that is needed to disable card readers and exit requests in any given area. First responder personnel can still gain access to the area if their record is marked with "executive privilege".
- The Controller should be able to adapt access rights to a change in condition or "threat" levels. Each personnel record should be assigned a clearance level for each area to which they have

access. When the condition is more severe than the person's clearance level then access is automatically denied. The Condition Level may be set manually through workstation or automatically through a program. A program can even be used to monitor national threat levels and adjust Condition Levels accordingly.

- Each controller should support the use of two expansion modules plus an Display unit. The expansion module is used for expanding the controller for special or access to doors. Modules can also be used to provide a cost effective entry reader only solution.

- The Access controller should support up to 32 Infinet nodes. The RS-485 programmable port can be set to support a wired or wireless Infinet field bus.

- The Controllers should be ready to support a wide range of card formats. Ideal for retrofits, The Controller lets you preserve existing cards by accepting standard formats (Weigand, ABA, HID Corporate-1000, CardKey) as well as custom formats (Custom Weigand, Custom ABA). The Controller should support formats up to 260-bits making the controllers ready for government installations that must meet HSPD-12 and FIPS 201 standards.

- SNMP (Simple Network Messaging Protocol) messages may be sent to network monitoring software to inform IT managers as to the health and presence of the access controller on the corporate network. The Access Controller should also support the SNMP alarming option.

Fire & Smoke Detection System

Fire can have disastrous consequences and affect operations of a Control Room. It is required that there is early-detection of fire for effective functioning of the Control Room.

i. System Description

The Fire alarm system shall be an automatic 1 ton (e.g. 8) zone single loop addressable fire detection and alarm system, utilizing conventional detection and alarm sounders.

Detection shall be by means of automatic heat and smoke detectors located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

ii. Control and Indicating Component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of EN54 Part 2 for the control and indicating component and EN54 Part 4 for the internal power supply.

- All controls of the system shall be via the control panel only.

- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.

- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.

- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify command.

iii. Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

iv. Smoke detectors

Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 7 and be LPCB approved. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

v. Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of EN54 Part 5 and be LPCB approved
- The detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.

vi. Addressable detector bases

- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

vii. Audible Alarms

Electronic sounders shall be coloured red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

viii. Commissioning

The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

ix. High Sensitivity Smoke Detection System

General – The HSSD system shall provide an early warning of fire in its incipient stage, analyse the risk and provide alarm and actions appropriate to the risk. The system shall include, but not be limited to, a Display Control Panel, Detector Assembly and the properly designed sampling pipe network. The system component shall be supplied by the manufacturer or by its authorized distributor.

x. Regulatory Requirements

- National Electrical Code (NEC)
- Factory Mutual
- Local Authority having Jurisdiction

Precision Air Conditioner

#	Parameters	Specifications
1.	Capacity	2 Ton
2.	Type	Precision
3.	Star Rating	5 star
4.	Energy Saving	Yes
5.	Temperature Control	Yes
6.	Cooling Capacity	above 5000 W
7.	Compressor Type	Rotary/ Scroll
8.	Compressor Warrantee	5 Years
9.	Air Circulation CFM (H/M/L)	above 500/450/300
10.	Moisture Removal L/Hr	above 1.8
11.	IDU Noise Level(DBA)	<=55/50/45
12.	Control	Microprocessor controlled cordless remote
13.	Power Source (V/Hz/ Φ)	230/50/1
14.	Display	LED/LCD
15.	Remote Control Distance	min. 10 meter
16.	Input Voltage	130-300 V
17.	Output Voltage	240 +/- 5 percent
18.	High Voltage Cutoff	240V
19.	Efficiency	>95 percentage
20.	Frequency	50 Hz
21.	Operations Design	24 x 7
22.	Air Discharge	Through EC Plug Fan
23.	Blower	Dual Blower for flexibility of operations and better redundancy
24.	Coolant	R410A / R407C Refrigerant
25.	Thermostat	Safety thermostat with manual reset feature must be provided
26.	Humidifier	Electrode Type / Infrared

Air Conditioner for City Management Room (17 TR)

#	Parameter	Specifications
1.	Product Type	Ceiling Concealed Duct
2.	Indoor Unit Noise Level (H/M/L)	67 / -- / -- dB(A)
3.	Operation Range	Up to 53°C
4.	Energy saving (zero power consumption, standby mode)	Yes
5.	Refrigerant Type	R22
6.	E.S.P (External Static Pressure) Control	Yes
7.	Two Thermistors Control	Yes
8.	Cooling Capacity in TR	17
9.	Air Flow Rate (H/M/L) (CFM) - Indoor Unit	6900
10.	External Static Pressure	12 mmAq
Out Door Unit		
11.	Compressor Type	Scroll
12.	Sound Level (H)	71 dB(A)
13.	Piping Connections (Liquid)	Ø 15.88 mm
14.	Piping Connections (Gas)	Ø 34.93 mm
15.	Drain(Outdoor/Indoor)	Ø 25.4 / 22.6 mm
16.	Max. Piping Length (Main Piping)	30M

Comfort Air Conditioner

#	Parameter	Specifications
1.	Capacity	2 TON
2.	Energy Efficiency	5 Star
3.	Energy Efficiency (EER (Cooling, W/W))	3.51
4.	Noise Level (Indoor, High/Low, dBA)	45/28
5.	Noise Level (Outdoor, High/Low dBA)	54
6.	Power Source(Φ/V/Hz)	1/230/50
7.	Power Consumption(Cooling, W)	Avg. 2000
8.	Operating Current(Cooling, A)	8
9.	Piping Length (Max, m)	30
10.	Piping Height (Max, m)	15
11.	SVC Valve (Liquid (ODxL))	6.35
12.	SVC Valve (Gas (ODxL))	15.88
13.	Moisture Removal (l/hr)	2.5
14.	Air Circulation (Cooling, m^3/min)	21
15.	Refrigerant (Type)	R410A
16.	Low Ambient (Cooling, °C)	16 ~ 52
17.	Outdoor Unit (Compressor Type)	BLDC
18.	Outdoor Unit (Anti-Corrosion Fin)	Yes

#	Parameter	Specifications
19.	Outdoor Unit (Multi-Channel Condenser)	Yes
20.	Air Direction Control (Up/Down)	Auto

UPS for CCC with 30 Minutes Back Up

#	Parameter	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at respective location (25+ KVA or more)
2.	Output Wave Form	Pure Sine wave
3.	Input Power Factor at Full Load	>0.90
4.	Input	Three Phase 3 Wire for over 5 KVA; 415 / 230 V; Frequency – 50 Hz ± 3 Hz
5.	Input Voltage Range	305-475VAC at Full Load
6.	Input Frequency	50Hz +/- 3 Hz
7.	Output Voltage	400V AC, Three Phase for over 20 KVA UPS
8.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)
9.	Inverter efficiency	>90%
10.	Over All AC-AC Efficiency	>85%
11.	Crest factor	Min. 3:1 at full load
12.	Noise level	< 55 db @ 1 Meter
13.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1)Output over voltage 2)Output under voltage 3)Battery low 4)Inverter overload 5)Over temperature 6)Output short
14.	Battery Backup	60 minutes in full load
15.	Battery	VRLA (Valve Regulated Lead Acid)
16.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.
17.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
18.	Cabinet	Rack / Tower type
19.	Operating Temp	0 to 65 degrees centigrade

#	Parameter	Minimum Specifications
20.	Management Protocol	SNMP Support through TCP/IP
21.	Protection	To be provided for overload/ short circuit; overheating; input over/ under voltage; output over/ under voltage.
22.	Certification	ISO 9001:2008 & ISO 14001 certified
23.	Compatibility	UPS to be compatible with DG Set supply and mains supply
24.	Safety Certificate	IEC 62040-1

Lighting

#	Parameter	Minimum Specifications
1.	Overhead Lighting	All overhead lighting shall be LEDs both recessed direct and indirect lighting including pot-lights.
2.	Aesthetics	The overhead lighting treatment shall be incorporated into the other ceiling elements to create an aesthetic specialty ceiling design in combination with the rooms.
3.	Lighting Intensity	Overhead lighting intensity shall be ✓ Command & Control Centre – at least 400 lux ✓ City Operations Center – at least 400 lux ✓ War Room – at least 500 lux ✓ Server Farm Area – at least 500 lux ✓ UPS Room – at least 5090 lux ✓ IBMS Room / Enclosure – at least 5900 lux ✓ NOC Room – at least 500 lux
4.	Dimming Control	✓ Dimming Control shall be continuous (all lights dimmable) and zone based (with minimum of 4 lighting zones on separate circuits. ✓ Dimming Control shall have various configurations preset for ideal operations lighting environment, based upon the perimeter glass wall natural lighting conditions (e.g. sunny, cloudy, partly cloudy night, etc.) ✓ Dimmers shall not be ganged in one box.
5.	Switching	✓ Manual switches shall be used for on / off lighting control and for overriding any preset lighting configurations ✓ Cover plates for switches shall match the colour of the switches, receptacles and receptacle cover plates.
6.	Quality	✓ All lighting fixtures shall be of high-grade quality over and above the standard level of quality for office lighting. ✓ Lighting shall be configured in order to reduce glares and

#	Parameter	Minimum Specifications
		reflection on console monitors and on the video wall, as well as accommodate any other lighting needs the monitors and video wall may have.
7.	Arrangement	Lighting arrangement shall accommodate console locations

CAT 6 Cables

#	Parameter	Minimum Specifications
1.	Environmental Space	Plenum
2.	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, AEX / EBU, Digital Video, RS-422, Noisy Environments, 250 MHz Category 6
3.	AWG Size	23
4.	Material	FEP – Fluorinated Ethylene Propylene
5.	Outer Shield Material	Aluminium Foil Polyester
6.	Drain Wire Material	TC – Tinned Copper
7.	Outer Jacket Material	LS PVC – Low Smoke Polyvinyl Chloride
8.	Cabling	Patented Central X-spline
9.	Conductor DCR	9.38 Ohm/100m
10.	Capacitance	160 pF/100m
11.	Installation Temp. Range	0°C to +50°C
12.	UL Temp. Rating	75°C
13.	Storage Temp. Range	-20°C to +75°C
14.	Operating Temp. Range	-20°C to +75°C
15.	Bulk Cable Weight	44 lbs./1000 ft.
16.	Max. Recommended Pulling Tension	25 lbs.
17.	Min. Bend Radius / Minor Axis	1.0 Inch
18.	Min. Bend radius Installation	2.25 Inch
19.	ANSI Compliance	S-116-732-2013 Category 6, ANSI/NEMA WC-66 Category 6

#	Parameter	Minimum Specifications
20.	Telecommunication Standards	ANSI/TIA-568-C.2 Category 6
21.	IEEE Specifications	POE per 802.3af & POE+ per 802.3at-2009

WiFi for ICCC Building

WiFi should confirm to the following internationally accepted standards

- ✓ 802.11 – Pertains to wireless LANs and provides 1 - or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- ✓ 802.11a – an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- ✓ 802.11b – 802.11 high rate WiFi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- ✓ 802.11g – Pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

10.10 Schedule – X (City Management Center - Surveillance System)

PTZ Dome Camera for Indoor Surveillance

S. No.	Parameter	Minimum Specifications
1.	General Requirements	The camera should be based upon standard components and proven technology using open and published protocols
2.	Image Sensor with WDR	True WDR 90 db or better, 1/2.8' Progressive CMOS Sensor or better with minimum 2 MP resolution
3.	Resolution	Camera should be Full HD PTZ 1920 (w) x1080 (h)
4.	Frame Rate	Shall support up to 25/30 fps
5.	Lens specs	Auto-focus, 4.4 –120mm (corresponding to 25x) or better
6.	Minimum illumination	Colour: 0.5 lux, B/W: 0.1 lux (at 30 IRE) or better
7.	Pre-set Positions	256 or better, Pre-set tour
8.	PTZ	Pan: 0 to 360° endless/continuous, 0.2 to 300°/s (auto), 0.2 to 100°/s (Manual) Tilt: 90°, 0.2 to 100°/s (Auto), 0.2 to 40°/s (Manual) 20x optical zoom and 10x digital zoom

S. No.	Parameter	Minimum Specifications
9.	General	The camera shall be able to setup and stream out minimum two (2) stream profiles. Each stream profile can have its own compression, resolution, frame rate and quality independently
10.	Outdoor Protection	The camera should be complete with IP 66 rated housing, Connectors, Camera Mounts, Power Supply and all Ancillary Equipment & all accessories
11.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, 802.1X, IPv4/v6, QoS, DNS, DDNS, NTP
12.	Compression Capability	H.265/H.264 compression with 3 Mbps and lower bitrate at 1920 X 1080 @ 30 FPS per stream and MJPEG
13.	Noise Reduction	DNR (2D/3D)
14.	Certificate	CE, UL, FCC, ONVIF
15.	Industry Standards	ONVIF S Compliant
16.	Miscellaneous	Power Supply: External 12V /24V/48V DC/ POE+
17.	Ethernet	Connectors: 10Base-T/100Base-TX
18.	Miscellaneous	Cable routing through base or rear of housing or feed through
19.	Miscellaneous	Operating conditions unit: -10° C to 50° C or better, humidity 20% to 90% non-condensing
20.	Miscellaneous	Tamper Proof
21.	Miscellaneous	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
22.	Audio	Audio capture Capability
23.	Local Storage	SD Card Slot with minimum 64 GB Class 10 SD card and expansion 128 GB
24.	Security	Password Protection, HTTPS encryption, IEEE 802.1X
25.	S/N Ratio	≥ 50dB
26.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
27.	Mounting Accessories	For pole and surface mount with L/C Brackets
28.	IR Illumination	Internal/External > 150 meters

Fixed Dome Camera for Indoor Surveillance

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.265
2.	Video Resolution	1920 X 1080
3.	Frame rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate
4.	Operating frequency	50 Hz
5.	Image Sensor	1/3” Progressive Scan CCD / CMOS

#	Parameter	Minimum Specifications or better
6.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
7.	Lens	5-50mm IR corrected, CS-mount lens, P-Iris
8.	Electronic Shutter	1/28000 s to 2 s or better
9.	Multiple 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
10.	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 m
11.	IR Cut Filter	Automatically Removable IR-cut filter
12.	Day/Night Mode	Yes with IR Cut Filter
13.	S/N Ratio	≥ 50 dB
14.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
15.	Wide Dynamic Range	True WDR 120 db or better
16.	Privacy Masks	Minimum 20 configurable 3D zones
17.	Audio	Full duplex, line in and line out, G.711, G.726
18.	Local storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
19.	Edge Storage	SD Card Slot with minimum 64GB Support Class 10 speed
20.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G
21.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
22.	Intelligent Video	Motion Detection & Tampering alert
23.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface

#	Parameter	Minimum Specifications or better
24.	Operating conditions	-10 degree C to 65 degree C
25.	Interface	RJ 45, 100 Base TX
26.	Humidity	Humidity 10–95% RH (condensing)
27.	Casing	NEMA 4X / IP-66 rated & IK 09
28.	Certification	UL2802 / EN, CE ,FCC, IEC
29.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at Compliant
30.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
31.	Support	The system should not be an end of life / end of service product.
32.	White Balance	Auto / Manual
33.	Back Light Compensation	Auto
34.	Functional	Self-cleaning / anti-dust / hydro-phobic coating features
35.	Mounting Accessories	For pole and surface mount with L/C Brackets
36.	IR Illuminator	External / build-in IR Illuminator with minimum 50 mtr.

10.11 Schedule –XI (Data Center)

Network Racks / Server Racks

#	Parameter	Minimum Specifications
1.	Type	• 19” 42U racks mounted on the floor • Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. • All racks should have mounting hardware 2 Packs, Blanking Panel. • Stationery Shelf (2 sets per Rack) • All racks must be lockable on all sides with unique key for each rack • Racks should have Rear Cable Management channels, Roof and base cable access

#	Parameter	Minimum Specifications
2.	Wire managers	Two vertical and four horizontal
3.	Power Distribution Units	• 2 per rack • Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground & Output to Ground
4.	Doors	• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. • Front and Back doors should be perforated with at least 63% or higher perforations. • Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.
5.	Fans and Fan Tray	• Fan 90CFM 230V AC, 4" diameter (4 Nos. per Rack) • Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor
6.	Metal	Aluminium extruded profile
7.	Side Panel	Detachable side panels (set of 2 per Rack)
8.	General	✓ Dual 32 A PDU ✓ 16 Receptacle Power Connectors each connected to separate PDU

Servers

#	Parameter	Minimum Specifications
1.	Processor	✓ Latest series/ generation of 64 bit x86 processor(s) with Ten or higher Cores ✓ Processor speed should be minimum 2.4 GHz ✓ Minimum 2 processors per each physical server
2.	RAM	Min. 24 DIMM slots, should be provided with 256 GB RAM using DDR4 DIMM's operating at 2666 MT/s (depending on processor model)
3.	Internal Storage	2 x 400 GB SAS (10k rpm) hot swap disk with extensible bays

#	Parameter	Minimum Specifications
4.	Network interface	2 X 20GbE LAN ports for providing Ethernet connectivity Optional: 1 X Dual-port 16Gbps FC HBA for providing FC connectivity
5.	Power supply	Dual Redundant Power Supply
6.	RAID support	As per requirement/solution
7.	Operating System	Licensed version of 64 bit latest version of Linux/ Unix/Microsoft® Windows based Operating system)
8.	Form Factor	Rack mountable/ Blade
9.	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE and Citrix.
10.	Storage controller	SAS Raid Controller with RAID 0/1
11.	Bus Slots	Minimum of 2 Nos of PCIe 3.0 based mezzanine slots supporting Converged Ethernet adapters
12.	Motherboard	Intel Chipset compatible with the offered processor
13.	Interfaces	Minimum of 1 Internal USB 3.0 port, 1 Internal SD Card Slot
14.	Redundancy	Must have port level and card level redundancy
15.	Operating System & Virtualization Support	✓ Microsoft Windows Server (latest version) ✓ Red Hat Enterprise Linux (RHEL) (latest version) ✓ SUSE Linux Enterprise Server (latest version) ✓ VMware / feature rich virtualization software supporting solution design & stack
16.	Warranty	5 Year OEM Warranty

Blade Chassis Specifications

The blade chassis shall have the following minimum technical specifications:

1) Minimum 6U size, rack-mountable, capable of accommodating minimum 8 or higher hot pluggable blades
2) Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided
3) Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy.
4) Have the capability for installing industry standard flavors of Microsoft Windows, and Enterprise RedHat Linux OS as well as virtualization solution such as VMware.
5) DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades allowing remote installation of software
6) Minimum 1 USB port

7) Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality

8) Two hot-plugs/hot-swap redundant 16 Gbps Fiber Channel module for connectivity to the external Fiber channel Switch and ultimately to the storage device

9) Hot plug/hot-swap redundant power supplies to be provided, along with power cables

10) Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.

11) Required number of PDUs and power cables, to connect all blades, Chassis to Data Center power outlet.

12) Hot pluggable/hot-swappable redundant cooling unit

13) Provision of systems management and deployment tools to aid in blade server configuration and OS deployment

14) Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.

15) Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP

16) Dedicated management network port shall have separate path for remote management.

17) Blade chassis shall be Electronic Industries Alliance Standard width rack mountable and provide appropriate rack mount kit

18) Enclosure should support full height / width and half height / width blades in the same enclosure, occupying a maximum of 10U rack height and it should support minimum 8 blade servers

19) Enclosure should be populated fully with power supplies of the highest capacity and energy efficiency of Platinum rating

20) 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)

21) 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.

22) Enclosure should support all Intel Xeon scalable processors based 2 CPU and 4 CPU blades

23) Should support built-in management software in redundancy

24) Should support single management console for all the blade servers across multiple chassis.

25) Solution should support templates to quickly make changes to the infrastructure, 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.

26) Requires 5 year OEM Warranty

Firewall

#	Item	Minimum Specifications
1.	Physical attributes	• Should be mountable on 19" Rack • Modular Chassis /Appliance Design • Internal redundant power supply
2.	Interfaces	• Should have minimum 4X1GE ports and 2X10G port with necessary SFP loaded from day one. Should be scalable to add 2 or more 10G ports in future. • Console Port 1 number
3.	Performance and Availability	• Encrypted throughput: minimum 2 Gbps • Concurrent connections: up to 100,000 • Simultaneous VPN tunnels: 2000
4.	Routing Protocols	• Static Routes • RIPv1, RIPv2 • OSPF
5.	Protocols	• TCP/IP, PPTP • RTP, L2TP • IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for Ipv6 • IPSEC
6.	Other support	• 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS, Support multilayer firewall protection, Traffic shaping, Bandwidth monitoring
7.	QoS	• QoS features like traffic prioritization, differentiated services, committed access rate. Should support for QoS features for defining the QoS policies.
8.	Management	• Console, Telnet, SSHv2, Browser based configuration • SNMPv1, SNMPv2 , SNMPv3
9.	Additional Features	• Should have inbuilt HDD of minimum 64 GB • Should support DDoS protection

#	Item	Minimum Specifications
10.	Certifications	ICSA/NDPP/EAL4

IPS (Intrusion Prevention System)

#	Item	Minimum Specifications
1.	Performance	Should have an aggregate throughput of no less than 200Mbps Total Simultaneous Sessions – 10,000
2.	Features	IPS should have Dual Power Supply IPS system should be transparent to network, not default gateway to Network IPS system should have Separate interface for secure management IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.
3.	Real Time Protection	• Web Protection • Mail Server Protection • Cross Site Scripting • SNMP Vulnerability • Worms and Viruses • Brute Force Protection • SQL Injection • Backdoor and Trojans • DoS/DDoS attack
4.	Stateful Operation	• TCP Reassembly • IP Defragmentation • Bi-directional Inspection • Forensic Data Collection • Access Lists
5.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from database server on web Device should have capability to define User Defined Signatures
6.	Block attacks in real time	• Drop Attack Packets • Reset Connections • Packet Logging • Action per Attack
7.	Alerts	• Alerting SNMP • Log File • Syslog • E-mail

#	Item	Minimum Specifications
8.	Management	• SNMP V1, V2, V3 • HTTP, HTTPS • SSHv2, Telnet, Console
9.	Security Maintenance	• IPS Should support 24/7 Security Update Service • IPS Should support Real Time signature update • IPS Should support Provision to add static own attack signatures • System should show real-time and History reports of Bandwidth

Network Switch

#	Parameter	Minimum Specifications
1.	Ports	• 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports • All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.
2.	Switch type	Layer 3
3.	MAC	Support 8K MAC address.
4.	Backplane	56 Gbps or more Switching fabric capacity (as per network configuration to meet performance requirements)
5.	Forwarding rate	Packet Forwarding Rate should be 70.0 Mpps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
8.	Protocols	• Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • Support based on 802.1p priority bits with at least 8 queues • DHCP support & DHCP snooping/relay/optional 82/ server support • Shaped Round Robin (SRR) or WRR scheduling support. • Support for Strict priority queuing & Sflow • Support for IPV6 ready features with dual stack • Support upto 255 VLANs and upto 4K VLAN IDs
9.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication
10.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private

#	Parameter	Minimum Specifications
		VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent
11.	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number
12.	Management	• Switch needs to have RS-232 console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface

EMS (Enterprise Management System)

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

- Network Monitoring System
- Server Monitoring System
- Helpdesk System

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

- **Network Management System**

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

Solutions should comply with The International Organization for Standardization (ISO) network management model defines five functional areas of network management

The ISO network management model's five functional areas are listed below.

- Fault Management—Detect, isolate, notify, and correct faults encountered in the network.
- Configuration Management—Configuration aspects of network devices such as configuration file management, inventory management, and software management.
- Performance Management—Monitor and measure various aspects of performance so that overall performance can be maintained at an acceptable level.
- Security Management—Provide access to network devices and corporate resources to authorized individuals.
- Accounting Management—Usage information of network resources

The solution should have also capable of following features

- The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- The system should be able to clearly identify configuration changes and administrators should receive an alert in such cases.
- **Server Performance Monitoring System**
    - The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
    - The proposed tool must provide information about availability and performance for target server nodes.
    - The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
- **Centralized Helpdesk System**
    - Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA’s pertaining to incident resolution time for priority / non-priority incidents.
    - System should also automatically create tickets based on alarm type
    - The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident via web interface for issues related to the project.
    - The solutions should capable of more proactive and preventing future incidents through visibility and analysis of past experience
    - The solutions should completely comply with latest ITIL standard framework

Storage

#	Parameter	Minimum Specifications
1.	Capacity	• 500+ TB
2.	Solution/ Type	• IP Based/iSCSI/FC/NFS/CIFS
3.	Storage	• Storage Capacity should be as per Overall Solution Requirement (usable, after configuring in offered RAID configuration) • RAID solution offered must protect against double disc failure. • Disks should be preferably minimum of 3 TB capacity • To store all types of data (Data, Voice, Images, Video, etc.) • Storage system capable of scaling vertically and horizontally
4.	Hardware Platform	• Rack mounted form-factor • Modular design to support controllers and disk drives expansion
5.	Controllers	• At least 2 Controllers in active/active mode with NSPoF Architecture • The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades. • Storage should support non-disruptive online firmware upgrade for both Controllers and disk drives.
6.	RAID support	• RAID 0, 1, 1+0, 5+0, 6+0 and 10 (Dual parity or higher)
7.	Disk drive support	Storage subsystem shall support 4TB/6TB/8TB or higher NLSAS/SATA/equivalent 7.2K drives in the same device array.
8.	Cache	• Minimum 128 GB of useable cache across all controllers. If cache is provided in additional hardware for unified storage solution, then cache must be over and above 128 GB.
9.	Redundancy and High Availability	• The Storage System should be able to protect the data against single point of failure with respect to hard disks, connectivity interfaces, fans and power supplies
10.	Management software	• All the necessary software (GUI Based) to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots etc. are to be provided for the entire system proposed. • Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in in the future, upto max capacity of the existing

#	Parameter	Minimum Specifications
		controller/units. • A single command console for entire storage system. • Should also include storage performance monitoring and management software • Should provide the functionality of proactive monitoring of Disk drive and Storage system for all possible disk failures • Should be able to take "snapshots" of the stored data to another logical drive for backup purposes
11.	Data Protection	The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for up to 4 hours
12.	Converge	Storage converge solution with NSPoF (No Single Point of Failure) Architecture. The storage solution should support NAS and SAN as an integrated offering with high availability at each level. The architecture should allow upgrades of hardware and software for investment protection.
13.	Protocols	Solution should be configured with required protocols for the solution CIFS / SMB 3 / NFS4 / iSCSI / FCoE / FC. All required protocols required for the solution to be enabled.
14.	Operating System	The storage array should support operating system platforms and clustering on Windows / Linux
15.	Cache Memory	Each controller / node should be provided with appropriate ARM scalable to 512 GB RAM with usable protected data cache for disk IO operations. If NAS controller with separate controllers is provided then additional RAM cache to be provided. The storage array must have complete cache protection mechanism either by de-staging data to disk / flash or protected with NVRAM.
16.	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 number of disks configured, as per system architecture best practices.
17.	Thin Provisioning	Proposed array must be supplied with Thin provisioning for the configured capacity.
18.	De-Duplication	Should provide de-duplication functionalities for the configured capacity.
19.	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.

#	Parameter	Minimum Specifications
		Snapshot should support both block and file..
20.	Replication	Storage array must have the capability to do remote replication using IP Technology.
21.	Software Licenses	All necessary software and licenses to configure and manage storage space, RAID configuration, Logical Drive allocation, Snapshots, compression, de-duplication, replication, auto-tiering for the configured capacity to be provided from day 1.

SAN Switch

The overall design of the safe should be suitable for safe storage of computer diskettes, tapes, smart c

#	Item	Minimum Specifications
1.	Converge	Fibre switch should be quoted with minimum 48 FC ports of 16 Gbps speed with all supported licenses from day one.
2.	Protocols	Switch should have support for 8 / 16 Gbps HBA
3.	Controllers	Switch should have auto sensing, zoning, integrate Ethernet and serial port for communication
4.	Operating System	Switch should be rack mountable 1U size and should be supplied with mounting kit
5.	Cache Memory	Switch should be equipped with redundant hot swap power supply and fan and allow hot swap ability with resetting the switch or affecting the operations of the switch
6.	Host	Switch should be backward compatible
7.	Connectivity	Switch should be capable for non-disruptive firmware upgrade and hot code activation
8.	RAID Supports	Switch should be capable of end to end performance monitoring
9.	Redundancy	Switch should have support for POST and online / offline diagnostics, non-disruptive daemon restart FC ping and path info (FC trace route)
10.	Disk Drive Support	Switch should be capable to interface with host based adapters (HBA) of multiple OEM, supporting multiple operating systems
11.	Global Hot Spare	Switch should have zoning and security features – hardware & software ACL and Policy based security & centralized fabric management
12.	Support	✓ Secure access ✓ FC based authentication ✓ RADIUS, SSH, SNMP ✓ Port Binding ✓ Port Masking ✓ Hardware based inter switch linking / trunking

#	Item	Minimum Specifications
		✓ Dynamic load balancing of links with no overhead ✓ Web based management and should support CLI ✓ Alert based on threshold value for temperature, fan status, power supply status and port status ✓ Shall support different port type such as FL port, F Port, M Port (mirror port), 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
13.	Licenses	All relevant licenses for all the defined features and scales

Fire proof enclosure

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

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

Core Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.
4.	Interface modules	Must support upto 10G interfaces. Must have capability to interface with variety interfaces.
5.	Protocol Support	Must have support for TCP/IP, PPP Frame relay and HDLC Must support VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, and BGP. Support IPV4 & IPV6
6.	Manageability	Must be SNMP manageable

#	Item	Minimum Specifications
7.	Scalable	• The router should be scalable. For each slot multiple modules should be available. • The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future.
8.	Traffic control	Traffic Control and Filtering features for flexible user control policies
9.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
10.	Remote Access	Remote access features
11.	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis • All interface modules, power supplies should be hot-swappable
12.	Security features	• MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS Authentication • Management Access policy • IPSec / Encryption • L2TP
13.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate

Internet Routers

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces
2.	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements.
3.	Interface modules	Must support up to 10G interfaces as per the design. Must have capability to connect with variety of interfaces.
4.	Protocol Support	• Must have support for TCP/IP, PPP, X.25, Frame relay and HDLC • Must support VPN

#	Item	Minimum Specifications
		• Must have support for integration of data and voice services • Routing protocols of RIP, OSPF, and BGP. • Support IPV4, IPV6 • Support load balancing
5.	Manageability	Must be SNMP manageable
6.	Traffic control	Traffic Control and Filtering features for flexible user control policies
7.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement
8.	Remote Access	Remote access features
	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis • All interface modules, power supplies should be hot-swappable
9.	Security features	• MD5 encryption for routing protocol • NAT • URL based Filtering • RADIUS/AAA Authentication • Management Access policy • IPSec / Encryption • L2TP
10.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate

Server Load Balancer

S. No.	Specification
1.	Device should support load balancing of both TCP and UDP based traffic using algorithms like round robin, weighted round-robin, least connections, persistent connects, etc.
2.	Device should provide minimum throughput of 10Gbps
3.	Device should provide 4x10G ports scalable to additional 4x10G ports
4.	Should support Client availability (Heartbeat) monitoring
5.	Should be support High Availability in Active-Active, Active-Passive mode.
6.	Should be Manageable using CLI(SSH), WebUI(SSL), SNMP (V1, V2, V3), etc.
7.	The management option should allow configuration, operation, firmware upgrade, traffic reporting, error logs, status logs
8.	Should support IPv6 from day one
9.	Should support static and dynamic routing
10.	Should support Global Server Load balancing, URL based Load balancing, HTTP, HTTP redirection, HTTP Layer 7 redirection, DNS redirection, DNS Fallback redirection,

S. No.	Specification
11.	Should be able to create and load http/SSL certificates
12.	Should be Rack mountable & should be supplied with Indian standard AC power cord.
13.	Should support multiple instances having dedicated CPU, memory, SSL & I/O for guaranteed performance.

L3 Switch

#	Item	Minimum Specifications
1.	Ports	✓ 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports / FX Ports (splits as needed) and extra 2 number of Base-SX / LX ports ✓ All ports can auto-negotiate between 10 Mbps / 100 Mbps / 1000 Mbps, half duplex or full duplex and flow control for half duplex ports
2.	Switch Type	Layer 3
3.	MAC	Support 8K MAC Address
4.	Backplane	✓ 56 Gbps or more switching fabric capacity for 24 ports ✓ 104 Gbps or more switching fabric capacity for 48 ports
5.	Forwarding Rate	Packet forwarding rate should be 70 Mbps or better
6.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
7.	Flow Control	Support IEEE 802.3x flow control for full duplex mode ports
8.	Protocols	✓ Support 802.1D, 802.1S, 802.1w, Rate limiting ✓ Support 802.1X Security standards ✓ Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping ✓ 802.1p Priority Queues, port mirroring, DiffServ ✓ Support based on 802.1p priority bits with at least 8 queues ✓ DHCP support and DHCP snooping / relay / optional 82 / server support ✓ Shaped Round Robin (SRR) or WRR scheduling support ✓ Support for IPV6 ready features with dual stack ✓ Support up to 255 VLANs and up to 4K VLAN IDs ✓ Support IGMP snooping and IGMP Querying ✓ Support Multicasting ✓ Should support lip protection and Loop detection ✓ Should support ring protection
9.	Access Control	✓ Support port security ✓ Support 802.1x (Port based network access control) ✓ Support for MAC filtering

#	Item	Minimum Specifications
		✓ Should support TACACS+ and RADIUS authentication
10.	VLAN	✓ Support 802.1Q Tagged VLAN and port based VLAN and Private VLAN ✓ Switch must support dynamic VLAN Registration or equivalent ✓ Dynamic Trunking protocol or equivalent
11.	Protocol & Traffic	✓ Network Time Protocol or equivalent Simple Network Time Protocol support ✓ Switch should support traffic segmentation ✓ Traffic classification should be based on user definable application types : TOS, DSCP, Port based, TCP/UDP port number
12.	Management	✓ Switch needs to have RS-232/USB console port for management via a console terminal or PC ✓ Must have support SNMP v1, v2 and v3 ✓ Should support 4 groups of RMON ✓ Should have accessibility using Telnet, SSH, Console Access, easier software upgrade through network using TFTP, etc. Configuration management through CLI, GUI based software utility and using web interface.

L2 Switch

#	Minimum Specifications
1.	19" Rack Mountable stackable switch with min 24 Nos. 10/100/1000 copper input POE/PoE+ (15.4W) ports and additional support of 4x1G SFP, support for external/internal redundant power supply.
2.	Switch should support for minimum 96 Gbps of forwarding throughput & minimum 70 mbps forwarding rate
3.	The switch should support dedicated stacking port separate from uplink ports with 80 Gbps of stacking bandwidth to put minimum 8 switches into a single stack group.
4.	Switch should have static, default IP routing enabled from day one.
5.	Switch shall have IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk.
6.	It shall have IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP or equivalent technology and static routes.
7.	Switch should have feature to protect access ports using port security, TACACS/TACACS+, Radius, storm control, Access Control List both port, VLAN based.
8.	Switch should have queuing as per IEEE 802.1P standard on all ports with mechanism for traffic shaping and rate limiting features for specified Host, network, Applications etc.

#	Minimum Specifications
9.	Should have Power supply 230 Volt 50Hz input
10.	The switch should support IPv6 Guard, IPv6 RA-Guard, IPv6 DHCP- Guard, Source-Guard features
11.	Switch should support automated image installation, configuration & automatic configuration of per port QoS to reduce switch provisioning time & effort.
12.	Must have SNMP v1, v2, v3 from day one
13.	Should have CLI and GUI based management console port.
14.	The switch should support IEEE 802.3az from day-1
15.	The switch should be IPv6 ready
16.	The proposed switch should be EAL2/ NDPP certified by common Criteria body at the time of delivery.

Tape Drive

S. No	Item	Minimum Specifications
1	Make	Must be specified
2	Model	Must be specified. All relevant technical information/brochures must be submitted
3	Technology	LTO 6
4	Number Drives	Two LTO 6 Drives
5	Media Slots	Minimum 45
6	Interface	Minimum 4 Gbps FC Interface
7	Power Supplies	Redundant Hot Swap Power supply
8	Fans	Redundant Hot Swap cooling fans
9	Software	Security and Remote Management Software
10	Supported Backup Software	Should support industry leading backup software such as Symantec Net Backup or any other suitable
11	Accessories	With all required cables and accessories to install and configure in standard 19” rack and to connect to Server/SAN switch

Backup Software

#	Specification
1.	The software shall be able to back up the necessary and relevant video feeds from storage, various databases, etc.
2.	Should support file level backup/recovery
3.	Should perform Scheduled unattended backup using policy-based management for all Server and OS platforms
4.	The software should support on-line backup and restore of various applications and Databases

#	Specification
5.	Should support database platforms like Microsoft Exchange Server, Oracle, Microsoft SQL Server, Microsoft SharePoint, Sybase, MySQL, Informix, IBM Domino (Lotus), SAP, IBM DB2, etc.
6.	Should support backup hardware like tape, virtual tape, optical, disk, interface hardware, etc.
7.	The backup software should be capable of having multiple back-up sessions simultaneously
8.	The backup software should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots
9.	The backup software should support different types of user interface such as GUI, Web-based interface
10.	Should have logging and reporting features

Centralised Antivirus S/w

- Shall be able to scan through several types of compression formats.
- Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- Shall be able to scan only those file types which are potential virus carriers (based on true file type)
- Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls
- Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- The solution must support multiple remote installations
- Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- Should be capable of providing multiple layers of defence.
- Shall have facility to clean, delete and quarantine the virus affected files.
- Should support in-memory scanning so as to minimize Disk IO.
- Should support heuristic scanning to allow rule-based detection of unknown viruses
- Updates to the scan engines should be automated and should not require manual intervention
- All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
- Updates should be capable of being rolled back in case required

- Should support various types of reporting formats such as CSV, HTML and text files
- Shall be able to automatically push any updates, patches, fixes to all client machines to ensure up-to-date antivirus protection for all IT devices and systems.

Directory services

- Should be compliant with LDAP v3
- Support for integrated LDAP compliant directory services to record information for users and system resources
- Should provide authentication mechanism across different client devices / PCs
- Should provide support for Group policies and software restriction policies
- Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
- Should provide support for X.500 naming standards
- Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
- Should support directory services integrated DNS zones for ease of management and administration/replication.

KVM Module

#	Item	Minimum Specifications
1.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Center
2.	Form Factor	19” rack mountable
3.	Ports	minimum 8 ports
4.	Server Connections	USB or KVM over IP.
5.	Auto-Scan	It should be capable to auto scan servers
6.	Rack Access	It should support local user port for rack access
7.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations
8.	OS Support	It should support multiple operating system
9.	Power Supply	It should have dual power with failover and built-in surge protection
10.	Multi-User support	It should support multi-user access and collaboration

10.12 Schedule –XII (Network Bandwidth)

Bandwidth (For Edge Equipment)

S.N.	Parameter	Description /Minimum Specifications
1.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol
2.	Bandwidth	1680 Mbps (total)
3.	Physical Connectivity	Wired Underground
4.	SLA	99.99 Uptime

Primary & Secondary Bandwidth (For ICCC to Safe City)

S.N.	Parameter	Description /Minimum Specifications
1.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol
2.	Bandwidth	1 Gbps
3.	Physical Connectivity	Wired Underground
4.	SLA	99.99 Uptime

Primary & Secondary Internet Bandwidth at ICCC

S.N.	Parameter	Description /Minimum Specifications
1.	Connectivity Type	MPLS L2/L3 , MPLS Cloud Should Support IP Multicast, PIM, BGP and OSPF protocol
2.	Bandwidth	500 Mbps
3.	Physical Connectivity	Wired Underground
4.	SLA	99.99 Uptime

10.13 Schedule –XIII (Field Elements & Accessories)

PTZ Camera out-door

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.265
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min 25 fps
4.	Operating frequency	50 Hz
5.	Image Sensor	1/3" OR ¼" Progressive Scan CCD / CMOS
6.	Lens	Auto-focus, 4.3 – 129 mm (corresponding to 30 X) PIRIS Lens
7.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.265 individually configurable
8.	Minimum Illumination	Colour: 0.05 lux, B/W: 0.01 lux (at 30 IRE, F 1.2) or better
9.	Day/Night Mode	Colour, Mono, Auto
10.	Wide Dynamic Range	True WDR 120 db or better
11.	S/N Ratio	≥ 50dB
12.	PTZ	Pan: 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) 30 optical zoom and 10x digital zoom Pre-set tour 256 preset positions, Tour recording, Guard tour
13.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, , Electronic Image Stabilization
14.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G
15.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
16.	Local Storage	Minimum 64 GB Memory card in a Memory card slot. In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
17.	Intelligent Video	Motion Detection & Tampering alert
18.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface
19.	Operating conditions	0 to 50°C
20.	Casing	NEMA 4X / IP-66 rated & IK10
21.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at

#	Parameters	Minimum Specifications or better
		Compliant
22.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS
23.	Certifications	UL/EN,CE,FCC, ONVIF
24.	IR Illumination	Internal > 150 meters

Fixed Outdoor Box/Bullet Camera

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.265
2.	Video Resolution	1920 X 1080
3.	Frame rate	50 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate
4.	Operating frequency	50 Hz
5.	Image Sensor	1/3" Progressive Scan CCD / CMOS
6.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
7.	Lens	5-50mm IR corrected, CS-mount lens, P-Iris
8.	Electronic Shutter	1/28000 s to 2 s or better
9.	Multiple 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
10.	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 m
11.	IR Cut Filter	Automatically Removable IR-cut filter
12.	Day/Night Mode	Yes with IR Cut Filter
13.	S/N Ratio	≥ 50 dB
14.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
15.	Wide Dynamic Range	True WDR 120 db or better
16.	Privacy Masks	Minimum 20 configurable 3D zones
17.	Audio	Full duplex, line in and line out, G.711, G.726

#	Parameter	Minimum Specifications or better
18.	Local storage	microSDXC up to 64GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
19.	Edge Storage	SD Card Slot with minimum 64GB Support Class 10 speed
20.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & preferably G
21.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption, IEEE 802.1Xa network access control, Digest authentication, User access log
22.	Intelligent Video	Motion Detection & Tampering alert
23.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface
24.	Operating conditions	-10 degree C to 65 degree C
25.	Interface	RJ 45, 100 Base TX
26.	Humidity	Humidity 10–95% RH (condensing)
27.	Casing	NEMA 4X / IP-66 rated & IK 09
28.	Certification	UL2802 / EN, CE ,FCC, IEC
29.	Power	802.3af PoE (Class 0) and 12VDC/24AC/ / POE+ IEEE 902.3at Compliant
30.	Physical security	Detection of camera tampering and Detection of Motion should be possible using either camera or VMS

Environmental Sensors

S.N.	Parameter	Minimum Specification
1	General	• They should be ruggedized enough to be deployed in open air areas such as Traffic Junctions, Streets, Parks, Parking Lots etc. • The sensor should be able to communicate its data using wireless technology • The data should be collected in a software platform that allows third party software applications to read that data. • The sensor management platform should allow the configuration of the sensor to the network and also

S.N.	Parameter	Minimum Specification
		location details etc.
2	Measurement component	Temperature, Humidity, Ambient Light, Sound, CO, NO2, NOX, CO2, SO2
3	Measurement range	• NO2: 0 to 10 ppm • NOX : 0 to 50ppm , 5000ppm • SO2 : 0 to 500 ppm • CO : 0 to 1000 ppm • O3: up to 1000 ppb • CO2 : 0 to 5% (5000 ppm) • PM 2.5: 0 to 230 micro gms / cu.m • PM 10: 0 to 450 micro gms / cu.m • Light: up to 10,000 Lux • UV: up to 15 mW/ cm2 • Noise: up to 120 dB (A) • Temperature : 0 to 100° C
4	Repeatability	±0.5% FS
5	Zero Drift	±1.0% FS max./week ±2.0% FS/week max. if range is less than 200ppm ±2.0% FS max./month for O2 Meter
6	Temperature and Humidity Sensor	• Real-time Temperature Range: 0ºC ~ 70ºC • Real-time in Air Humidity Level Display (up to 100%)
7	Span drift	±2.0% FS max./week ±2.0% FS max./month for O2 meter
8	Response speed	60 seconds max. for 90% response from the analyzer Inlet
9	Connectivity & Data Interface	USB / Ethernet /Wireless (GPS ,GSM, Wi-Fi- 802.11 n/ac)
10	Operating Temperature	0 to 55 °C

Public Addressal Systems

S.N.	Parameter	Minimum Specification
1	PAS System	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously. The PAS should also support both, Live and Recorded inputs
2	Speaker	Minimum 2 speakers, To be used for Public Address System
3	Connectivity	IP based
4	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
5	Integration	with VMS and Command and Control Centre
6	Construction	Cast Iron Foundation and M.S. Pole, Sturdy Body for equipment

S.N.	Parameter	Minimum Specification
7	Battery	Internal Battery with different charging options (Solar/Mains)
8	Power	Automatic on/off operation
9	Casing	IP-66 rated for housing
10	Operating Conditions	-10° to 65°C

Panic Button & Emergency Call Box

S. No.	Parameter	Specification
1	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment
2	Call Button	Watertight Push Button, Visual Feedback for button press
3	Speaker	To be used for Public Address System
4	Connectivity	GSM/PSTN/Ethernet as per solution offered
5	Sensors	For tempering/Vandalism
6	Battery	Internal Battery with different charging options (Solar/Mains)
7	Power	Automatic on/off operation
8	Casing	IP-66 rated for housing
9	Operating conditions	-10° to 65°C

Digital VMD

#	Specifications	Minimum Requirements
1	Location	To be installed at locations identified by Authority and the text on the sign must be readable even in broad daylight
2	LED Type	DIP
3	Pixel Configuration	1R/1G/1B
4	Pixel Density	10000 dots/m2
5	Environmental Grade	UV Resistant
6	Colour	True Colour
7	Brightness & Legibility	○ To be read even in broad daylight without any shade ○ The displayed image shall not appear to flicker to the normal human eye ○ >6000 cd/m2
8	Luminance Class	L-3 as per EN 12966
9	Contrast Ratio	R2-R3 as per EN 12966
10	Beam Width	B6+ : Viewing angle shall ensure message readability for citizens, motorists, pedestrians, etc. on the respective

#	Specifications	Minimum Requirements
		locations
11	Best Viewing Distance	10m – 100m
12	Display capability	○ Fully programmable, full colour, full matrix, LED displays ○ Alpha-numeric, Pictorials, Graphical & video
13	Display Language	To support both pictograms and bilingual (English and Punjabi) text
14	Display Front Panel	It shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean 100% anti-glare
15	Message Creation	Through both a Central Control Room Application and a local Laptop/Device loaded with relevant software
16	Language	Multilingual (Punjabi/English/Hindi) and all fonts supported by windows
17	Auto Dimming	Auto dimming adjusts to ambient light level.
18	In built Sensor	Photoelectric sensor
19	Storage capacity	Minimum 60 GB
20	Display Area	Customized (2.88m x 1.96m with 5-10% tolerance)
21	Number of Lines & Characters	The number of lines and characters can be customized as per the requirement (Min 3 Lines & 10 Characters)
22	Brightness & contrast	Controlled through software
23	Display Driving method	Direct current control driving circuit. Driver card of display applies Direct Current Technology
24	Display Style	Steady, flash, partial flash, right entry, left entry, top entry, bottom entry, canter spread, blank, and dimming
25	Connectivity	IP Based
26	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.
27	Integration	○ Interface with GPRS or Ethernet ○ Integration with Command and Communications Center and service providers for offering G2C and B2C services
28	Construction	Mounting structure shall use minimum 6 Mtrs. high hexagonal/octagonal MS Pole or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.
29	Battery	○ 230VAC+ 15%, 50Hz, Single Phase (automatically re-start in the event of an electricity supply failure) ○ Batteries with solar charging options can also be recommended as back up

#	Specifications	Minimum Requirements
30	Power	Automatic on/off operation
31	Casing	○ Weather-proof Display for VMS ○ IP-66 rated for housing all control equipment
32	Operating conditions	-10° to 65°C
33	Message Validity	If the controller is unable to connect to the server for the next message, it shall not display the old message, which has passed its expiry time. Instead it shall be programmed to display a default message.

Application Software for VMD (Control Messaging Application at Data Center)

The Application System for Controlling Messaging for VMD shall:

1) Be deployable over multiple (3 to 4) workstations.

2) Ensure that provision for feeding/updating the following information:

A. VMD messages and information
B. Types of possible scenarios per VMD
C. Types of possible messages to be displayed on each VMD during various scenarios

3) Ensure that the normal operator users are not able to publish any custom message and shall only display predefined sets of messages.

4) 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.

5) Ensure that users can publish specific messages for managing traffic and also general informative messages.

6) Allow an operator to seamlessly toggle between multiple VMD points at each workstation in order to send specific messages to specific locations.

7) Accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client.

VMS (Video Management Software)

#	Specifications	Minimum Requirements
1.	General	• The VMS should be built on "Open Platform" i.e. should be able to support any ONVIF compliant IP cameras without any limitation to any kind of licensing. • VMS server shall be deployed in a clustered server environment/Support in built for high availability and failover for directory & recording servers • VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.

#	Specifications	Minimum Requirements
		• All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). • The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map • The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
2.	Scalability	The VMS shall have ability to connect and integrate other technologies and third party software systems (e.g. ANPR, RLVD, Face Detection, Speed Violation Detection, Environmental Sensors etc.) and act as a singular platform for entire surveillance and security system. The system should be able to bi-directionally and dynamically exchange data between various software applications in real-time as well as schedule transfer. It should Support for unlimited cameras, servers, sites and clients. Support for storage expandability.
3.	User Management	Centrally controlled user management - Users, roles, rules and privileges should be stored on the central VMS server allowing any authorized user to log into any workstation.
4.	Device Discovery	The VMS shall have ability to easily install, configure, modify, search and remove surveillance devices with automatic discovery of IP devices.
5.	Event Management	The VMS shall have ability to enforce custom settings for event detection, alarm notification, recording, input/out (I/O) control, and other features in response to events. The alarm management module shall support graphical displays with interactive icons to display the status of the cameras & other inputs.
6.	Software/Patch Upgrade	• The VMS shall have ability to enforce custom settings for event detection, alarm notification, recording, input/out (I/O) control, and other features in response to events. • The alarm management module shall support graphical displays with interactive icons to display the status of the cameras & other inputs. • For future requirement, migration to h.265 should happen with a simple firmware upgrade
7.	Recording & Transfer	- Should support dual streaming - Should allow each stream to be viewed independently by client viewer. - Recording from connected cameras Should be stored in individual databases. - Should support multiple storage formats - Should support recording in all resolution at desired FPS - Should support video cum audio recording - shall support automatic failover for recording

#	Specifications	Minimum Requirements
		- shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) - or Video Exports with VMS's Native Format along with Watermark and Encrypted with SSL / TSL technology, one can protect the video tampering and prove that the video is not tampered
8.	Motion Zone Masking	VMS should Support Exclusion of Motion /Masked Zones to enhances optimized recordings and storage.
9.	Customized Record Retention	Should support Customized recording retention period for specific camera, group, area etc.
10.	Remote User Support	Should support multiple remote users via network/web browser/client software
11.	Device Grouping	- The VMS shall have ability to logically group devices based on installation location, device type, configuration type or any other predefined rules. - Individual cameras/devices should have the capability to inherent rules from parent group/subgroup.
12.	Parameter Configuration	The VMS shall have ability to configure multiple streams with different quality parameters e.g. Codec (H.264, H.265 MPEG, JEPG) , resolution, frame & bit rate etc.
13.	Image Stabilization	The VMS shall have Electronic Image Stabilization feature
14.	Device Search	The VMS shall have ability to search and view device(s) based on standard criteria like ID, Name, Location, Group, Type etc.
15.	Storage Indexing	VMS should store video feeds in a standard folder tree structure so that it becomes easy for system admin to browse videos categories based on year, month, date and time wise. Also the file name should indicate important attributes like camera location, date, time etc.
16.	Video Wall /Monitor Support	- Multiple monitor support: The system should allow connecting multiple monitors on single client workstation and display different contents on each of the connected monitor. - All panes / tiles should indicate mode (live or recoded), source (camera name/location) and date/time and applied quality information (FPS, CODEC). - The font color shall be changed automatically in sync with the video/image to have a clear text reading at any point of time. - A matrix view should support multiple formats on video wall and any number of multiple screen divisions.
17.	PTZ Control	PTZ configuration and control including presets, patterns, patrolling, priority, Zoom in/out and permissions.
18.	Shortcut Keys	Along with menu-driven interface, a VMS should also support custom shortcut keys to helps operators quickly switch between

#	Specifications	Minimum Requirements
		different modules/screens, change views or panes/tiles and to carry out playback functions.
19.	Image Snapshot	System should allow creating a still image from live or recorded feed and storing it into a workstation.
20.	Digital Zoom	Digital zoom to enlarge portion of an image to provide superior zooming capability.
21.	Display Interface	Option to view surrounding cameras: The system should enable operators to select master camera feed and based on group/subgroup details, its surrounding cameras should be automatically displayed on separate panes. These panes/tiles should be dynamically generated so that operator does not need to manually pull the feeds from desired cameras.
22.	Video Search and retrieval	The VMS shall have ability to quickly search and retrieve recordings: Search methods should include search by camera(s), group, date/time, alarm/event / bookmark list, smart (motion) search by creating motion index or by generating thumbnail summary of a video archive to locate specific event.
23.	Playback Control	The system should offer following playback controls like Play/Pause, Lock speed, Forward playback (1x, 2x, 4x), Reverse playback (-1x, -2x, -4x), Slow forward playback (frame by frame, 1/8x, 1/4x,1/3x, 1/2x, 1x), Slow reverse playback
24.	Camera Tempering	The VMS should provide a centralized camera tampering detection solution in real-time by automatically identifying tampering to ensure video image capture and integrity. The solution sends an alert when the following potential tampering is detected: • Scene too bright — e.g. flash light, direct sun, laser pointer that is pointed at the camera, causing it to become over saturated. • Scene too dark — not enough light to see a clear image, if camera is covered. • Camera is covered or blocked — if something is blocking or partially blocking most of the camera’s field of view. • Camera redirection detection — if camera is redirected from its’ initial position of field of view (FOV). • Unfocused or blurred view — if the camera was sprayed with rain or its focus changed. The System should be able to detect tampering on any IP camera that has been discovered in the VMS
25.	Mobile App	The bidder needs to provide a Mobile App and integrate it with the VMS system for 2-way communication with the 10000 in a secure manner. The App should be able to provide Role-based access to the users
26.	Reports	The system should provide interactive reporting interface with standard and user-defined custom reports and filtering options to:

#	Specifications	Minimum Requirements
		- Review currently logged in users and functions being performed. - Retrieve audit trails - user activities, errors and system logs. - View list of hardware units and selected configuration options. - List down configured users and corresponding roles & permissions. - View details of bookmarks, event/alarm history and exported evidences.
27.	SDK	The VMS must be supplied along with its well documented Software Development Kit (SDK): The SDK should include a rich, easy-to-use Application Programming Interface (API) that supports the most common programming languages.

Video Analytics Application with licenses

Video analytics that shall be offered on identified cameras are

1. Parking Violation
2. Wrong/One-way detection
3. Triple riding
4. Helmet detection
5. No Number Plate Detection
6. Detection and classification of human, animal and vehicle
7. ‘Vehicle of interest’ tracking by colour, speed, number plate
8. Unwanted/ banned vehicle detection
9. Incident detection
10. Repeat offenders
11. Heavy vehicle no entry tracking
12. Stopped vehicle
13. Slow traffic/congestion detection
14. Crowd detection
15. Motion detection
16. Stopped pedestrian
17. Graffiti and Vandalism detection
18. Walking against mandatory flow/pedestrian movement
19. Unattended/abandoned object and tracking
20. Object Classification and facial recognition
21. Behavioral Biometry: Identification through multiple behavior (Optional)
22. Person climbing barricade
23. Person collapsing
24. Tripwire/Intrusion
25. Video fire detection
26. Target zone data for people or vehicles entering and remaining in target zone
27. Real-time scene analysis and counting data based on user definable rules
28. Camera based analytics for Traffic Management

a) Red Light Violation Detection
b) Automatic Number Plate Detection
c) Speed Violation Detection System
d) Face Recognition System

29. Camera based analytics for Solid Waste Management
a) Debris and Garbage detection
b) Attendance of sanitation workers on site by face recognition
c) Sweeping and cleaning of streets/bins before and after
d) Garbage bin, cleaned or not
e) Tracking of garbage truck movement and Quantity of garbage dumped at dumpsite

30. System functions and reports:
a) Reduce false alarms
b) Alarms to be sent to Voice, visual, relay closure, email, or cell phone alarm
c) Video/Camera events - signal lost and restored
d) Auditing
e) Customized alarm management
f) Rule based scene analysis and reports
g) Alarm Acknowledgement
h) MIS reports including Heat maps

#	Specifications	Minimum Requirements
1	General Requirement	The Video Analytics shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors
		Support any architecture namely distributed, centralized and hybrid
		Support system openness without using any proprietary format
		Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware
		Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation
		Able to process at variable resolution and frame rate when if necessary
		It shall support open platform Video Management System (VMS).
		It shall provide ONVIF device discovery
		It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client
		It shall stream the Analytics Video to VMS using open interface protocol like ONVIF.
		It shall support multiple regions of analytics on single video feed
		It shall support multiple features to be enabled for each of the regions
		It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time
		It shall support both Virtual line and Virtual area based features. The virtual area can be of any shape and can be bound by at least 10 end points.
		It shall support both indoor and outdoor environment.
		It shall support setting of minimum and maximum object size for detection.

#	Specifications	Minimum Requirements
		It shall support masking of area in a view
		It shall support object masking.
		It shall support color detection for vehicle & Object.
		It shall support alarms to filter based on object color, size, speed and aspect ratio.
		It shall support analytics capability to run both on server as well as edge (on camera).
		It shall support simultaneous running of different features both on edge as well as server for same camera
		It shall support camera independent licensing
		The System Should be capable to do the analytics on Live Video Cameras as well as Stored Video records from such cameras
2	Suspicious incident /Object detection	It shall detect person loitering in a virtual area for more than a pre-defined period.
		It shall detect crowd assembling in a pre-defined area. The count for the crowd determination should be pre-defined. It shall be able to provide live crowd count.
		The VA shall support dense and sparse crowds for crowd counting and crowd flow detection
		The VA shall detect object left out or abandoned in a virtual area by a person beyond a certain pre-defined period.
		The VA shall detect object removed by a person beyond a certain pre-defined period.
		The VA shall detect counter flow of people (such as people moving in a wrong way)
		Should be able to track a Person/ moving Object till the last point of the camera view
		The applications should also be able to do People search based on a given description/attributed/Sketch/Full length photograph
		Should have an interface to Create sketches, Composite (Human like Figure) of the suspect based on description. There Shall be different options available for describing hair color and style, Facial Attributes, shirts, trousers, patterns, etc.
3	Traffic Management Features	It shall detect vehicle or group of vehicle moving in a wrong way.
		It shall detect a vehicle parked in an area for a pre-defined period.
		It shall detect congestion due to vehicles
4	Other Features	It shall be able to stitch up to 4 camera videos with overlapped view and provide the stitched view.
		It shall be able to stabilize the video when camera is shaking (such as, due to wind) and shall be able to stream the stabilized video to VMS.

#	Specifications	Minimum Requirements
		Ability such that alerts can be searched and categorized based on this information. i. Timestamp (date & time) ii. Alert Name iii. Alert Type iv. Alert Location v. Text Description vi. Associated Region
		It shall provide video summary of all the alarms.
		It shall provide reporting option to export reports of alarms in PDF, EXCEL and Image formats and also option to schedule it.
		It shall support email and FTP of alarm data and also option to schedule it.
		It shall be able to provide comparison reports for different months and year

Industrial Grade 8 Port PoE+ Switch

#	Parameter	Minimum Specifications
1.	Enclosure Type	Desktop, rack-mountable 1U
2.	Subtype	Gigabit Ethernet
3.	Ports	4 x 10/100/1000 (PoE+) + 4 x 10/100/1000 (PoE) + 2 x combo Gigabit SFP
4.	Power Over Ethernet (PoE)	PoE+
5.	PoE Budget	180 W
6.	Performance	Forwarding performance (64-byte packet size): 38.69 Mpps Switching capacity: 52 Gbps
7.	Remote Management Protocol	SNMP 1,2,3, RMON 1,2,3,9 Telnet, HTTP, HTTPS
8.	Authentication Method	RADIUS, TACACS+
9.	Features	Flow control, layer 2 switching, BOOTP support, VLAN support, IGMP snooping, Syslog support, DoS attack prevention, port mirroring, DiffServ support, Weighted Round Robin (WRR) queuing, MAC address filtering, Broadcast Storm Control, IPv6 support, Multicast Storm Control, Unicast Storm Control, firmware upgradable, SNTP support, Spanning Tree Protocol (STP) support, Rapid Spanning Tree Protocol (RSTP) support, Multiple Spanning Tree Protocol (MSTP) support, Trivial File Transfer Protocol (TFTP) support, Access Control List (ACL) support, Quality of Service (QoS), MLD snooping, reset button, LLDP support, DHCP relay, DHCP client, Energy Efficient Ethernet, Generic Attribute Registration Protocol (GARP), Generic VLAN Registration Protocol (GVRP), Type of Service (ToS), 2 fans, 4.1MB packet buffer

10.	Compliant Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3at, IEEE 802.3az
11.	RAM	128 MB
12.	Flash Memory	32 MB
13.	Status Indicators	Port transmission speed, system, PoE, link/activity
14.	Expansion / Connectivity	
15.	Interfaces	4 x 1000Base-T - RJ-45 - PoE+ - 30 W
		4 x 1000Base-T - RJ-45 - PoE - 15.4 W
		2 x 1000Base-T - RJ-45
		2 x – SFP
17.	Power	
	Power Device	Internal power supply
	Voltage Required	AC 120/230 V (50/60 Hz)
18.	Environmental Parameters	
	Min Operating Temperature	-10 Degree C
	Max Operating Temperature	65 Degree C
	Humidity Range Operating	10 - 90% (non-condensing)

Online UPS for Field Components

#	Parameter	Minimum Specifications
1.	Capacity	1KV or more Line Interactive
2.	Technology	Automatic Voltage Regulation
3.	Input Frequency Range	50 Hz +/- 5%
4.	Output Frequency Range	50 Hz +/- 5%
5.	Output Voltage	180V AC - 280V AC Single Phase
6.	Input Voltage	230 VAC
7.	Voltage Regulation	+/-5% (or better)
8.	Output Waveform	True Sine Wave
9.	Output Power Factor	0.6 or more
10.	Battery Backup	Minimum backup of 1 Hour on full load
11.	Battery Type	VRLA (Valve-regulated Lead Acid battery)
12.	General Operating Temperature	-10 to 65 Degree Celsius
13.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery
14.	Bypass	Automatic, Manual Bypass Switch

#	Parameter	Minimum Specifications
15.	Optional SMPS	Power Management from SNMP manager and Web browser

Poles for Mounting Camera & Other SMART Components

#	Parameter	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713
2.	Height	5 Meter OR higher, As-per-requirements for different types of cameras & Site conditions.
3.	Pole Diameter	Bottom section : 97.9mm Middle Section : 76.2mm Top Section : 65.2mm
4.	Bottom base plate	Minimum base plate of size 30 x 30 x 15 cms
5.	Mounting facilities	Capable to Mount 3-4 Cameras, Environmental Sensors, PA Systems, ECB, and Digital Display boards with related Junction box.
6.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climatic conditions). Expected foundation depth of min. 100cms. Please refer to Earthing standards mentioned in RFP
7.	Protection	Lightning arrestors with proper grounding
8.	Sign-Board and Number-Plate	A sign board describing words such as “This area under surveillance” and with serial number of the pole.

Junction Box

#	Parameter	Specification
1.	Built	• The Outdoor Utility Cabinet will be constructed with a front sheet steel door with 3 point Locking system to ensure the security of the cabinet. Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet. • The Cabinet should have the required frames to mount the required components like, network device, power, edge router, UPS, LIU, battery, etc.
2.	Utility & IP rating	Should be Made for 24/7/365 Outdoor Applications; The Utility Cabinet shall be IP 66 rated (Regulatory Standard Compliance) for ingress protection.
3.	Size	The cabinet has to be provided of size suitable for the mounting of the associated network devices, power, and UPS, LPU/mini T server and Battery components securely and safely within the cabinet.
4.	Power Slot	3 x 5 way Indian Standard PDU’s has to be provided to support the site equipment. PDU type should be as per actual requirement.
5.	Installation	Each Cabinet will be mounted on a raised height Plinth, 600 - 1000 mm high, as per site requirements. FAN Cooling unit shall be inherent in the design.
6.	Cable Management	Proper cable management should be provided

#	Parameter	Specification
7.	Cable Routing:	Power connection cable shall be provided from the nearest access point to the Outdoor Utility Cabinet through Power meter enclosure.

Body Camera

#	Parameter	Specification
1.	Dimensions	95.9 mm x 52.2 mm x 27.6 mm (3.78" x 2.06" x 1.09") ±5%
2.	Weight	100-150 Grams
3.	Lens	f/2.0 , 130° wide angle
4.	Connection Interface	USB 2.0
5.	Storage	64 Gb or Higher
6.	Wi-Fi	Yes
7.	Bluetooth	Yes
8.	Microphone	Yes
9.	Battery Life (Fully Charged)	12 Hours or more
10.	Resolution	Full HD 1080P
11.	Frame Rate	30 FPS
12.	Video Compression	H.264/H.265
13.	Operating Temperature	-20°C (-4°F) ~ 65°C (149°F)
14.	Storage Temperature	-25°C (-13°F) ~ 70°C (158°F)
15.	IP Rating	IP67
16.	Viewing Angel	130° (diagonal)
17.	InfraRed	Built-in
18.	Required Accessories	USB cable/360° rotatable clip/Adapter/Velcro holder

Body Camera Docking Station

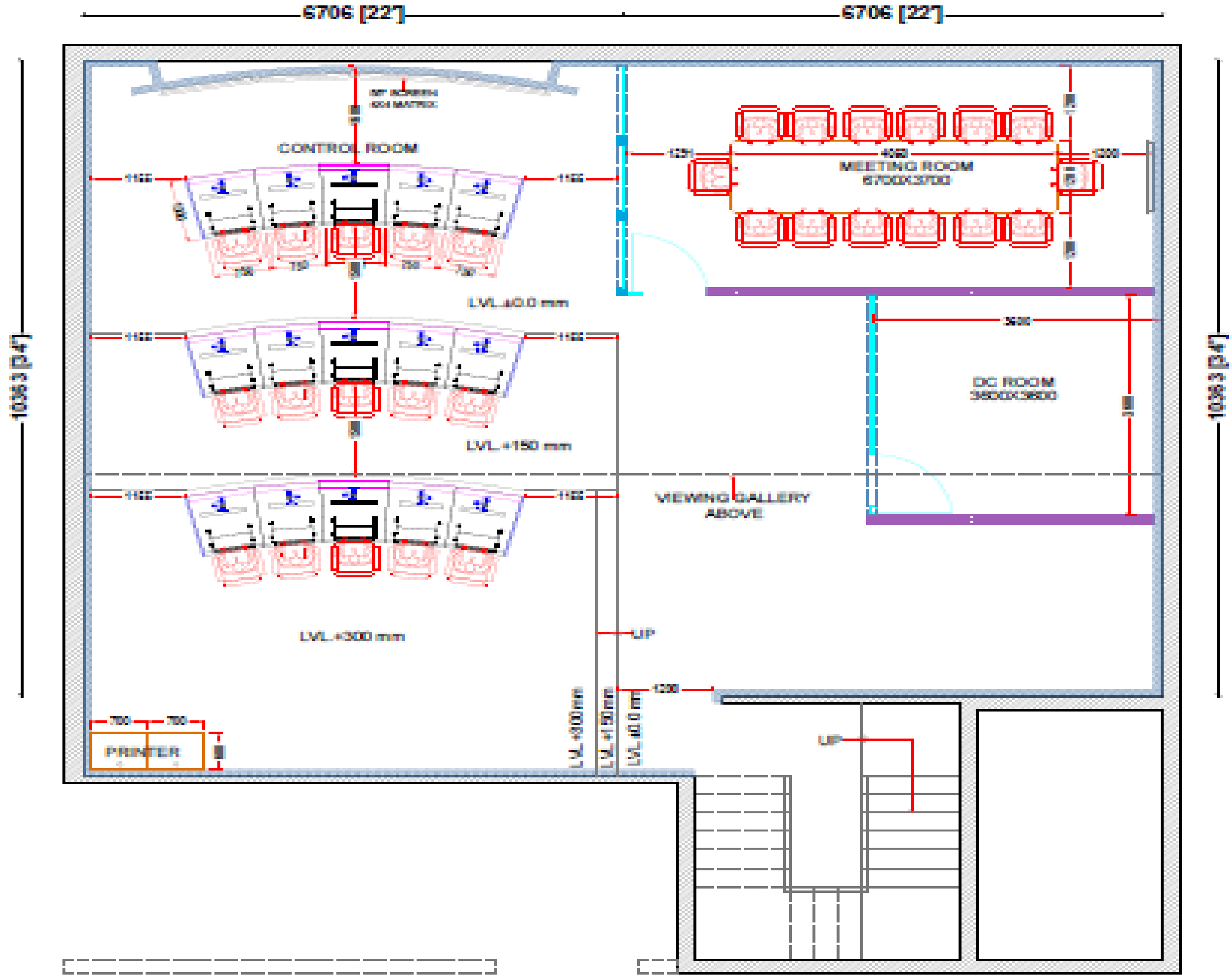
S.N.	Parameter	Specifications
1	Dimensions	(Max.)423 mm x 105 mm x 54 mm +/- 10%
2	Weight (Max.)	1000 Gram +/- 10%
3	Connection Interface	USB 3.0
4	Network Port	WAN: 10/100/1000 Mbps Ethernet LAN: 10/100 Mbps Ethernet
5	Operating Temperature	0°C (32°F) ~ 40°C (104°F)
6	Storage Temperature	-20°C (-4°F) ~ 70°C (158°F)
7	Power Supply (Max.)	19V / 3.42A
8	Certificate	CE/FCC
9	Operating System	Microsoft Windows 7, 8, 10
10	Camera docking capacity	6 or higher

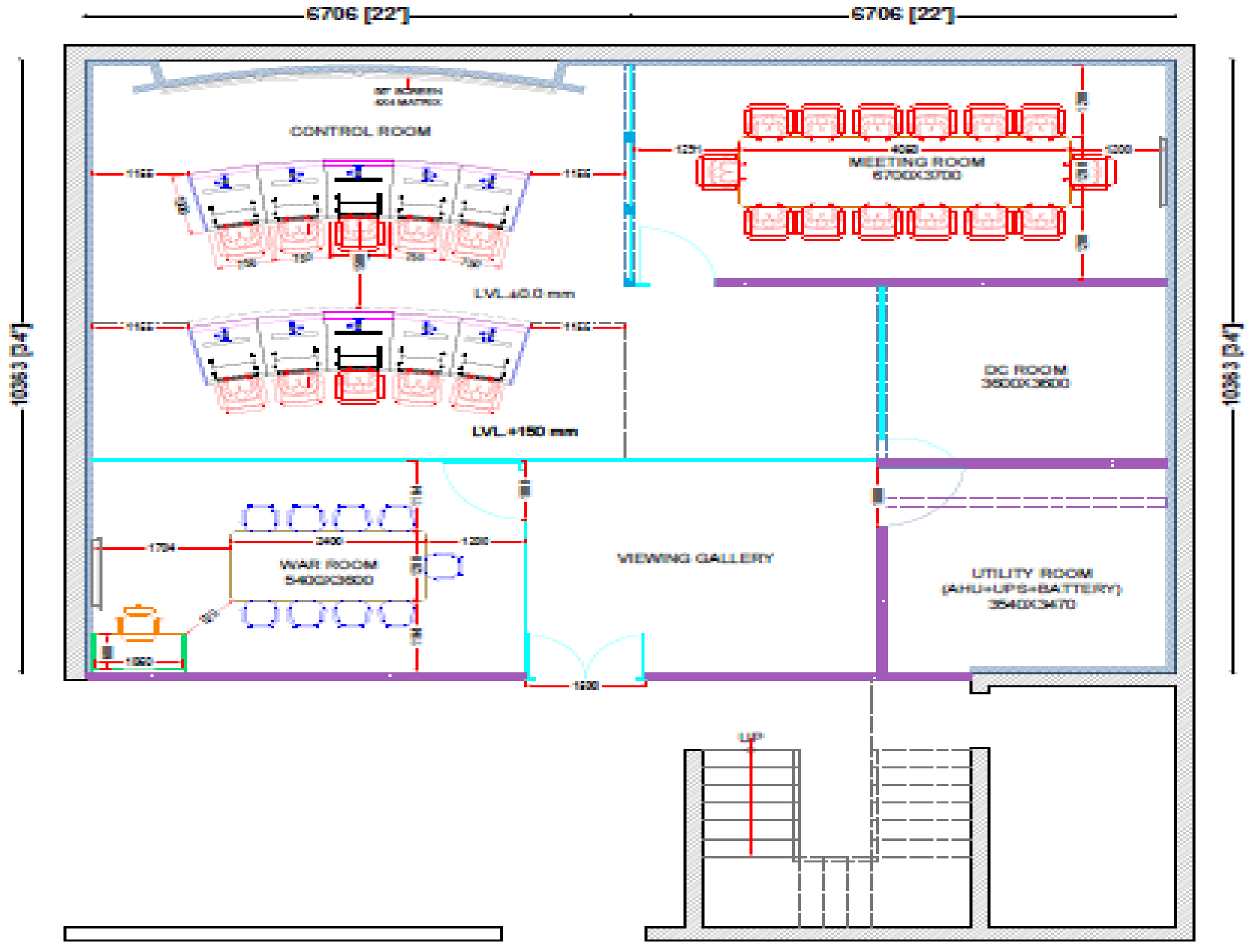
11. Indicative Floor Plan of CCC

The following table details the rooms and their respective sizes which form the part of Integrated Command and Control Centre (ICCC). Although it was decided earlier to host the ICCC in old Squash Court building, now it is being planned to host the ICCC in a new building getting planned by Ludhiana Municipal Corporation in Sarabha Nagar.

These dimensions and design are indicative only, bidder is allowed to propose any new layout or design which needs to be mutually discussed and agreed with Corporation at the time of execution.

S. No	Expenditure item	Area (Sq. Ft.)
1	City Operation Room	1,000
2	Meeting room	250
3	Contact center room	150
4	Technical support room	150
5	War room separated with glass glazing	300
6	Electrical room & Utility Room	150
7	Store room	100
8	Washrooms	100
9	Pantry	150
10	Entrance for telecom component (Fibre cabling etc.)	100
11	Conference room	250
14	Reception Area	100
15	Data Centre	200
Total Area (Approx.)		3000


6706 [22']
6706 [22']
10363 [34']
10363 [34']
CONTROL ROOM
1166
1166
LVL.±0.0 mm
LVL.+150 mm
LVL.+300 mm
MEETING ROOM
6700X3700
4060
1200
3600
DC ROOM
3600X3600
VIEWING GALLERY
ABOVE
UP
UP
1200
700
700
PRINTER
LVL.+300 mm
LVL.+150 mm
LVL.±0.0 mm


6706 [22']
6706 [22']
10363 [34']
10363 [34']
CONTROL ROOM
MEETING ROOM
6700X3700
4060
1200
DC ROOM
3600X3600
LVL.±0.0 mm
LVL.+150 mm
1166
1166
1166
1166
WAR ROOM
5400X3600
1704
2400
1200
1000
1500
VIEWING GALLERY
UTILITY ROOM
(AHU+UPS+BATTERY)
3540X3470
UP

13. Current Services/Module Status

S. No.	Modules	Present Automation Status	Planned Automation	Scope
1	Smart Lighting	No	Yes	Vendor Ob-boarding is already started for City Wide LED Light Replacement along with CCMS software. Total no of poles – 1,00,773 Municipal corporation – 24500 Electricity Department – 76000 (being included) No. of Lights- 1,05,000 Remote Command/Control at Feeder panel level ~1000 individual LED controls (future ready, iOT enabled) Feeder Panels – 1474 (need for one time replacement)
2	Solid Waste Management	Partial	Yes	Presently, GPS installed on 34 vehicles for tracking. Future expansion of GPS installation another 50 vehicles planned. CCTV Cameras Planned in MSI Contract as part of ICCC Project will be used to monitor Solid Waste Dump Sites
3	Smart Traffic	Partial	Yes	Presently, ANPR – 290 (Nos) and RLVD – 60 (Nos) planned to be installed by HFCL by Feb. However, ITMS to be discussed with client
4	City Bus ITMS	Yes	Yes	Presently, 160 buses are GPS enabled and CCTV cameras (approx. 3) are installed in the buses. Each bus is having a PA system installed for communication. There are 60 more buses planned in next 6 months. Currently, no control room provisioned
5	Environment Sensors	No	Yes	Part of MSI contract as part of ICCC Project

S. No.	Modules	Present Automation Status	Planned Automation	Scope
6	City Surveillance	Yes	No	The scope is as follows Fixed Box Camera – 935 (Nos) Pan Tilt Zoom Cameras (PTZ) – 155 (Nos) Automatic Number Plate Recognition (ANPR) – 290 (Nos) Red Light Violation Detection System (RLVD) – 60 (Nos) Video Management Software (VMS) - Owned by Polixel Video Analytics - Polixel Command and Control Centre - M3S Platform owned by Polixel Till now 1200 cameras has been installed in the City
7	Smart Governance	Yes		Detailed out in separate table
8	Smart Parking	No	Yes	2 MLCP are planned in next 2 years with total capacity of 1500 cars. Approx. 1500 sensors planned. Also, Public Bike sharing for 200 bikes/cycles are planned with GPS. Approx. 220 sensors planned
9	Water Scada	No	Yes	Presently, there is no sensor deployed at source, treatment, storage, distribution and House Service Connection. However, as per team discussions, approx 50 sensors to be implemented in ABD area of Ludhiana by AECOM on the above sources
10	Sewerage	Yes	Yes	Presently, Cameras are installed at 3 STP Locations
11	Power SCADA	Yes	Yes	Presently, 7 substations has been automated and another 43 substations planned in next 1 year. Control Centre is in Sarabha Nagar wherein, SCADA system is installed for monitoring of work stations
12	Panic Button & Emergency call box	No	Yes	Part of MSI contract as part of ICCC Project

S. No.	Modules	Present Automation Status	Planned Automation	Scope
13	Public Addressal System	No	Yes	Part of MSI contract as part of ICCC Project
14	Digital Variable Messaging Display	No	Yes	Part of MSI contract as part of ICCC Project

S. No.	Smart Governance Modules	Department	Implementing Agency	Implementation Year	Technology Stack	Type of Data	Data size per Sensor (since 2013)
1	Web Portal (www.mcludhiana.gov.in)	All Branches & Departments	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	0.8 GB
2	Building Completion Plan	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	More than 3 GB
3	Building Composition Fee	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
4	Building Plan Sanction (Commercial)	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
5	Building Plan Sanction (Industrial)	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
6	Building Plan Sanction (Others)	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
7	Building Plan Sanction (Residential)	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
8	Change of Land Use	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
9	Pollution N.O.C.	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
10	Refund of Extra Regularization Fee	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
11	Regularization of Plot/Colony	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
12	Birth Certificate Issue (Current)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
13	Birth Certificate Issue (Late Entry within one month)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
14	Birth Certificate Issue	Health Branch	Icon Software	2013	Asp.Net, SQL	Text,	

S. No.	Smart Governance Modules	Department	Implementing Agency	Implementation Year	Technology Stack	Type of Data	Data size per Sensor (since 2013)
	(Late Entry within one year)		Technologies		Server	Binary	
15	Birth Certificate Issue (NT) Maternal	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
16	Birth Certificate Issue (NT) Paternal	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
17	Birth Certificate Issue (Old)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
18	Correction in Birth Certificate	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
19	Correction in Death Certificate	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
20	Death Certificate Issue (Current)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
21	Death Certificate Issue (Late Entry within one month)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
22	Death Certificate Issue (Late Entry within one year)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
23	Death Certificate Issue (NT)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
24	Death Certificate Issue (Old)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
25	Inclusion of Child Name in Birth Certificate	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
26	Inclusion of Child Name in Birth Certificate (Current)	Health Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
27	CHANGE OF OWNERSHIP(BANK MORTGAGE)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
28	Change of Ownership(Court Case)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
29	Change of Ownership(Death Case-Natural Succession)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
30	Change of Ownership(Death Case-Registered Will)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	

S. No.	Smart Governance Modules	Department	Implementing Agency	Implementation Year	Technology Stack	Type of Data	Data size per Sensor (since 2013)
31	Change of Ownership(Death Case-UnRegistered Will)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
32	Change of Ownership(Sale Deed)	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
33	Correction in Property Particulars	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
34	New Property No	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
35	TS1 Copy	House Tax Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
36	Correction in Water Billing Particulars	Operation and Maintenance Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
37	New Sewage Connection	Operation and Maintenance Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
38	New Water Connection	Operation and Maintenance Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
39	Water and Sewage Connection	Operation and Maintenance Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
40	ADJUSTMENT/REFUND OF PROPERTY TAX	Property Tax	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
41	Correction in Property Tax Return	Property Tax	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	
42	Stock Inventory Management System	B&R, O&M, Health, Horticulture	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	0.5 GB
43	Property Tax Software	Property Tax / House Tax	Icon Software Technologies	2013	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	5 GB
44	Online Water & Sewerage Payment System	O&M, Water Sewerage, Health	Icon Software Technologies	2015	Asp.Net, SQL Server	Text, Binary	1 GB
45	Building Challan Management System	Building Branch	Icon Software Technologies	2013	Asp.Net, SQL Server	Text, Binary	0.4 GB

S. No.	Smart Governance Modules	Department	Implementing Agency	Implementation Year	Technology Stack	Type of Data	Data size per Sensor (since 2013)
46	Online Complaint System	All Branches & Departments	Icon Software Technologies	2013	Asp.Net, SQL Server, Android	Text, Binary	0.5 GB
47	Tower Management System	Building Branch	Icon Software Technologies	2016	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.2 GB
48	Tehbazari Management System Web Portal	Building Branch	Icon Software Technologies	2015	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.3 GB
49	Tehbazari Management System Android App	Building Branch	Icon Software Technologies	2015	Android, Java, SQL Server, Json, JavaScript etc.	Text, Binary	0.3 GB
50	Cow Cess Collection System	Health Branch	Icon Software Technologies	2017	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.2 GB
51	Online Trade License Fee collection System	Building Branch, Licensing Branch	Icon Software Technologies	2016	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.35 GB
52	Works Management System - Web Portal	B&R, O&M, Health, Horticulture	Icon Software Technologies	2014	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.2 GB
53	Works Management System - Android App	B&R, O&M, Health, Horticulture	Icon Software Technologies	2014	Android, Java, SQL Server, Json, JavaScript etc.	Text, Binary	0.2 GB
54	Patch Work Management System	B&R	Icon Software Technologies	2014	Asp.Net, SQL Server, Json, JavaScript etc.	Text, Binary	0.4 GB
55	Employee Information Management System	Personnel	Icon Software Technologies	2017	Asp.Net, SQL Server, Json,	Text, Binary	0.6 GB

S. No.	Smart Governance Modules	Department	Implementing Agency	Implementation Year	Technology Stack	Type of Data	Data size per Sensor (since 2013)
					JavaScript etc.		

Annexure 1 - Cyber Security Requirements for Ludhiana Smart City Project

a) Cyber Security Framework

The Bidder shall develop Cyber Security Framework aimed at building a secure and resilient cyberspace for citizens and stakeholders of Smart City. The Framework shall be designed to protect cyberspace information and infrastructure; build capabilities to prevent and respond to cyber-attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology. Framework shall cover smart city cyber security architecture with reference to the cyber security framework suggested by National Institute of Standards and Technology (NIST), CSA (Cloud Security Alliance) and ISO27001. Framework shall also comply with MoHUA, GoI Guidelines vide circular K- 1s016/6U2016-SC-1.

b) Cyber Security Policy

The Bidder shall ensure creation and implementation of Smart City Cyber Security Policy and related procedures in line with relevant international standards. The policy shall address security of hardware and software, along with the connectivity between the field device and the respective application software. The bidder shall ensure to develop and implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

c) Cyber Security Governance

1. The Bidder shall conduct Risk Assessment and prepare Risk Treatment Plan for the IT applications and infrastructure deployed in smart city ecosystem.
2. The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the smart city management.
3. The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed timelines.

d) Cyber Security Organization Structure

The Bidder shall clearly define Organization structure for Smart City Cyber Security with skilled personnel and adequate representation from Senior Management. The organization structure shall also include the roles and responsibilities of personnel deployed for cyber security of smart city.

The smart city cyber security resources shall be deployed as part of the team during the complete contract period i.e. implementation and operation stage.

e) Smart City IT Asset Management

The Bidder shall utilize automated asset management tools to prepare the information asset register (IAR) for all IT assets deployed in the Smart city. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.

The Bidder shall develop and implement an appropriate set of procedures for information labeling and handling in accordance with the classification scheme proposed in the cyber security policy of smart city.

f) Physical & Environmental Security

1. The bidder shall implement and manage physical security of IT assets of smart city, which shall include, as a minimum: locks, alarms, surveillance equipment, sensors, access control systems (biometrics), etc. The bidder shall also design processes and procedures for same.
2. The Bidder shall ensure that all the equipment, information or software shall not be taken off-site without appropriate authorization.

g) Access Control

1. The Bidder shall ensure that users shall be provided single sign on functionality if required for the applications and solutions deployed in Smart City.
2. The smart city solution should support multiple authentication methods such as Username password, two factor authentication, digital certificate and biometric based authentication.
3. 2FA solution should be capable of being deployed on mobile devices deployed for smart city
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The smart city solution should have the functionality to provide authentication based on the role.
6. Remote access to all smart city IT users shall be securely managed.
7. The smart city solution should be able to deploy and configure the approved password policy and should provide the feature to configure the logs.
8. The smart city solution should have the option of blocking multiple sessions for the user.
9. All smart city applications should support role based access control to enforce separation of duties.
10. The application deployed in smart city should display the last login status (successful/unsuccessful, time) to the user and should not store authentication credentials on client computers after a session terminates
11. All smart city solution should be compliant with Indian IT Act, 2000 and Amended IT Act, 2008

h) Communications and Operations Management

1. Bidders must ensure that the IT systems in the smart city infrastructure are open, scalable and interoperable. The deployed systems must operate within 4 layers – Sensory layer, communication layer, data layer and application layer adhering to relevant security controls as mandated by the MoHUA, GoI Guidelines.

2. Bidders shall ensure that all the interfaces between IoT devices, field sensors, device applications and storage deployed in smart city are encrypted using appropriate protocols, algorithm and key pairs.

3. All transport link communication must be encrypted and sensitive data both in rest and transit is to be secured using encryption.

4. Bidders must ensure that all the changes made to the smart city infrastructure incl. of IoT field devices, sensors and related applications should be tracked and recorded in order to enable security monitoring of the infrastructure. The maintained logs should be systematically collated, enabling the access of critical information as per date, fortnight, month, quarter, year etc.

5. Bidders should ensure that separate environments are maintained for production, test and development for smart city infrastructure and solutions to reduce the risks of unauthorized access or changes.

6. Bidders must ensure that smart city IT systems are designed in such a way that only authenticated users have access to the smart city database. Also, the provision of access has to be routed only through designated applications.

7. Bidders must ensure that sensitive data is stored in the smart city database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.

8. Bidders must ensure that the smart city architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications.

9. Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high level security monitoring of the smart city security infrastructure.

10. Bidders must ensure that the smart city components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the smart city.

11. Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the smart city infrastructure such as the data center, IoT device control room etc.

12. Bidders must ensure that platforms hosted in the central data center support multi-tenancy with adequate authentication and role based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges.

13. Bidders must ensure that the smart city architecture accounts for latency issues for the flow of data between devices. Suitable protocols should be utilized to minimize data flow latency upon management of heterogeneous data.

14. Bidders must strictly make sure that the communication between IoT field devices and their respective management applications happens only over a data layer (digital platform). Thereby enabling this designated layer to be the one true source of data abstraction, normalization and correlation.

15. Bidders must ensure that the smart city IT infrastructure including the Wi-Fi network adheres to relevant and applicable security standards and protocols. Also, bidders must make sure that the Application Program Interfaces (APIs) are published and the IT systems run on standard protocols.

16. Bidders must ensure that the smart city architecture end-to-end has adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.

17. Bidders must enable for wireless/ broadband architecture used in the smart city infrastructure to interface with other/citywide wireless networks thereby enabling interoperability.

18. Bidders must ensure that IoT field devices and sensory equipment operating within the smart city periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed.

19. Bidders must make sure that the wireless layer of the smart city network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa.

20. Bidders must enable for the authentication of the sensory equipment during the provisioning of the sensors and connection into the smart city infrastructure.

21. Bidders must ensure that the data aggregators used for enabling the interoperability between field IoT devices and sensors functioning on different protocols incorporate appropriate authentication and encryption at the aggregator gateway when field devices are not capable of authenticating /encrypting critical information.

22. Bidders must ensure that the IoT field devices and sensory equipment deployed in smart city periphery must not have a physical interface for administration. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed.

23. Bidders must ensure appropriate network segregation. The smart city data center must be systematically segmented into multiple zones. Each zone must have a dedicated functionality. IoT field devices and sensory equipment must be connected to a completely separate network isolated from public networks and other private networks.

24. Bidders must make sure that the internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined

ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data.

25. Bidders must ensure that Smart city data centres are well equipped with adequate security controls to protect the confidentiality, integrity and accessibility of critical data. The center should consider including cyber security systems such as firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioural analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity, access management system etc.

26. Bidders must ensure that the Smart city cyber security infrastructure incorporates high level security and monitoring controls such as SIEM (Security Information and Event Management) tools on all networks, field devices and sensors to identify malicious traffic.

27. Bidders must ensure all smart city applications must be hosted within India and must undergo static and dynamic security testing before deployment. Also, the applications must be periodically (at least once a year) tested for adequate security control.

28. Bidders must ensure that the proposed smart city architecture provides for:

    a. Automatic and secure firmware updates
    b. Device logging and auditing capabilities
    c. Vendor self-certification for non-existence of backdoors, undocumented and hard coded accounts.

29. Bidders must ensure that all the information on security incidents is regularly shared with Indian Computer Emergency Response Team (CERT-ln) and NCIIPC (National Critical Information Infrastructure Protection Centre) and their help is sought for appropriate mitigation and recovery from the security incidents.

30. Bidders shall ensure that Data encryption at rest shall be implemented using departments managed keys, which are not stored in the cloud.

31. The bidder shall setup Cyber Security Continuous Monitoring process to monitor - physical environment, External service provider activity etc. to detect potential cyber security incidents.

i) Information Systems Acquisition, Development and Maintenance

1. The Bidder shall prepare the detailed technical security requirement as part of the ‘Software Requirement Specification’ document with secure coding guidelines for development of applications for smart city.

2. The Bidder shall incorporate validation checks into smart city applications to detect any corruption of information through processing errors or deliberate acts.

3. The Bidder shall obtain information about technical vulnerabilities of information systems being used in smart city, evaluate the exposure to such vulnerabilities, and take appropriate measures to address the associated risk.

4. The bidder shall implement maintenance and repair process of smart city IT assets in timely manner, with approved and controlled tools.

j) Business Continuity Planning and Disaster Recovery

1. The Bidder shall implement and operate Disaster Recovery site for the Smart city infrastructure and related IT & OT applications. IT & OT applications and processes should be supported from the disaster recovery site.

2. The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a half yearly basis

k) Information Security Audits

The bidder shall ensure Information security audits of the smart city infrastructure and related applications by a CERT-In empanelled vendor. VA/PT (Vulnerability assessment and Penetration Testing) activities, audits and application security testing must be carried out on twice-a-year basis ensuring optimal operation and security of the smart city infrastructure and applications. Teams carrying out the audit exercise must be different from the implementation teams. Systematic actionable need to be derived post audits and necessary changes need to be made periodically.

l) Security Operations Center

The bidder shall set up Security Operations Centre to ensure continuous monitoring and manage all kinds of cyber security operations related to smart city such as Incident Management, Logging and Monitoring, Anti-virus Management, Threat Intelligence Support, Secure Technology Disposal and other cyber security support activities to ensure secured smart city ecosystem.

m) Awareness Training

The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and Availability of critical data.

n) Security Controls for Cloud Services

The security controls for creating and managing cloud services shall comply with the following guidelines.

Empanelment of Cloud Service Offerings CSPs facilities/services shall be compliant with regulative directives and industry best practices. The SLA shall be based on the guidelines issued by Government Departments on contractual terms related to Cloud Services (MeitY guideline dated 31/03/17). The security controls should include the following:

1. The CSP should be empanelled by MeitY for providing cloud services. The CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1 & PCI DSS.

2. The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.

3. The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC.

4. Incident Management shall be managed by CSP / third party.

5. Periodic secure code review shall be performed for cloud applications.

6. Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud.

7. The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.

8. CSP shall inform all security breach incidents to Smart City management on real time.

9. CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.

10. E-Discovery shall be included as clause in SLA with CSP. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.

11. The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP to perform all due diligence before releasing any such information to any such law enforcement agency.

12. CSP must ensure location of all data related to smart cities in India only.

13. The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MeitY guidelines. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.

14. CSP's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.

15. SLA with CSP shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.

16. Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined.

17. Change-management process (e.g., changes such as updates or new services) must be defined.

18. Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall to restrict access, Role based access management, Logging and monitoring shall be ensured.

19. VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.

20. Digital Certificate shall be implemented for secure access.

21. Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements; logging and monitoring should be enabled.

22. Application access between hosted smart city applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.

23. For SLAs to be used to steer the behaviour of a cloud services provider, imposition of financial penalties is to be incorporated.

24. Monitor Vendor Service level agreement for annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of six years form the date of operations of the systems.

Annexure 2- Plan Report on Cyber Security

XII Five-Year Plan on Information Technology Sector
Report of Sub-Group on Cyber Security

1.0 Background

Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. With the Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. It has also created new vulnerabilities and opportunities for disruption. The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

2.0 XI Plan – Objectives, targets and achievements

2.1 Objectives and Targets

The following primary objectives had been identified in XI Plan in cyber security:

- Securing cyber space
- Preventing cyber attacks
- Reducing national vulnerability to cyber-attacks.
- Minimizing damage and recovery time from cyber attacks
- Capacity building

As such, the cyber security initiatives in the XI plan period had the following focus:

- Enabling Legal Framework
- Security Policy, Compliance and Assurance
- Security R&D
- Security Incident – Early Warning and Response

- National Cyber Alert System
- CERT-In and Sectoral CERTs
- Information Exchange with International CERTs

- Security training o Skill & Competence development
    - Domain Specific training – Cyber Forensics, Network & System Security Administration
- Collaboration
    - International
    - National

2.2 Achievements during XI Plan

A number of activities have been performed in each of the above focus areas. Major achievements are summarised below:

2.2.1 Enabling legal framework

Information Technology (Amendment) Act, 2008 has been enacted and rules of important sections have been notified. The provisions of the Information Technology Act deal with evidentiary value of electronic transactions, digital signatures, cyber-crimes, cyber security and data protection.

2.2.2 Security Policy, Compliance and Assurance

Computer Security Guidelines have been circulated to all Departments and Ministries. Cyber security drills are being conducted to assess preparedness of critical organisations. 54 Auditors have been empanelled for audit of IT infrastructure from cyber security point of view.

Crisis Management Plan for countering cyber-attacks and cyber terrorism has been released and is being updated annually. Enabling workshops are being conducted in different sectors and states/UTs. Common Criteria (CC) product testing facility has been set up which caters up to level 4 CC certification.

Draft `National Cyber Security Policy’ has been prepared and posted on DIT website for public comments.

Controller of Certifying Authority (CCA) has licensed 7 Certifying Authorities (CA). More than 22 lakhs Digital Signature Certificates have been issued. Major Applications using Digital Signatures include e-Procurement for Central and State Govt., e-Tendering, e-Filing of returns (MCA-21), Income Tax filing for corporate and individuals, Interbank transactions (RTGS and SFMS), E-Filling of Patent Application and NSDL Applications.

2.2.3 Security Incident – Early Warning and Response

A Computer Emergency Response Team –India (CERT-In) has been set up and is operational as the national agency for cyber incidents. It operates a 24x7 Incident Response Help Desk to help users in responding to cyber security incidents. It has been issuing regular alerts on cyber security threats and advises countermeasures to prevent attacks. CERT-In has established linkages with international CERTs and security agencies to facilitate exchange of information on latest cyber security threats and international best practices. CERT-In, in collaboration with CII, NASSCOM and Microsoft, has created a portal “secureyourpc.in” to educate consumers on cyber security issues.

2.2.4 Cyber Security R&D

A number of R&D projects have been supported at premier academic and R&D institutions in the identified Thrust Areas, viz., (a) Cryptography and cryptanalysis, (b) Steganography, (c) Network & systems security assurance, (d) Network Monitoring, (e) Cyber Forensics and (f)Capacity Development in the area of cyber security. A host of Cyber Forensic tools have been developed in the country.

2.2.5 Capacity Development/Training

Training Centres have been set up at CBI, Ghaziabad and Kerala Police to facilitate advanced training in cybercrime investigation. Computer forensic labs and training facilities are being set up in J&K state, North Eastern states. Forensic Centres have been set up with the help of NASSCOM at Mumbai, Bangalore, Bhopal and Kolkata. Virtual training environment based training modules have been prepared. Training has been conducted for Orissa, Delhi, Andhra Pradesh and Karnataka Judicial Officers on Cyber Crime Investigation. 94 training Programmes have been conducted by CERT-In on specialized Cyber Security topics – in which 3392 people have been trained.

2.2.6 Collaboration

As part of National level Cooperation, Cyber security awareness programmes were organised in cooperation with industry associations – CII, NASSCOM-DSCI. MoUs were signed with product and security vendors for vulnerability remediation.

Several activities were undertaken under International Cooperation. International level Cyber security drills were held with Asia –Pacific CERTs. Specific cyber security cooperation agreements were signed with US, Japan and South Korea. India participated in cyber security drills of US (Cyber Storm III). CERT-In experts helped in establishment of CERT-Mauritius. India is participating in Internet traffic scanning in Asia-pacific region. India is a member of UN Committee of Group of Experts as well as in the Council of Security Cooperation in Asia-Pacific (CSCAP) for enhancing cooperation in the area of Cyber Security.

3.0 Current status of Cyber Security preparedness

The initiatives taken by the Government so far have focused on the issues such as cyber security threat perceptions, threats to critical information infrastructure and national Security, protection of critical information infrastructure, adoption of relevant security technologies, enabling legal processes, mechanisms for security compliance and enforcement, Information Security awareness, training and research. These actions have significantly contributed to the creation of a platform that is capable of supporting and sustaining the efforts to securing the cyber space. However, due to the dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time.

Salient features of the results of actions and the level of cyber security preparedness include:

(a) Information Technology (Amendment) Act 2008 has been enacted to cater to the needs of National Cyber Security by addressing host of issues such as technology related cybercrimes, critical information infrastructure protection, data security and privacy protection. Indian Computer Emergency Response Team (CERT-In) has been operational as a national agency for cyber security incident response. It has established operational linkages with overseas CERTs, and cyber security professional organisations to enhance its ability to respond to the cyber security incidents and take steps to prevent recurrence of the same.

(b) PKI infrastructure, set up to support implementation of Information Technology Act and promote use of Digital Signatures, has enabled the growth and application of digital signature certificates in a number of areas.

(c) National Crisis Management Plan for countering cyber-attacks and cyber terrorism has been prepared and is being updated annually. Central Govt. Ministries/Departments and States and UTs as well as organisations in critical sectors are making efforts to prepare and implement their own sectoral Crisis Management Plans.

(d) To enable comprehensive cyber security policy compliance, the Govt. has mandated implementation of security policy within Govt. in accordance with the Information Security Management System (ISMS) Standard ISO 27001. In addition, Computer security guidelines have been issued for compliance within Govt. A Common Criteria based IT product security testing facility has been set up at Kolkata, which can test IT products up to EAL4.

(e) A mechanism for audit and assessment of security posture of Govt. and critical sector organisations has been put in place. Security Auditors have been empanelled for conducting security audits including vulnerability assessment, penetration testing of computer systems and networks of various organizations of the government, critical infrastructure organizations and those in other sectors of the Indian economy. Cyber security drills are being conducted regularly to assess the preparedness of organisations to resist and mitigate cyber attacks.

(f) R&D activities have been supported through premier Academic and R&D Institutions in the country facilitating creation of R&D infrastructure, development skills and solution oriented development.

(g) Nation-wide Information Security Education and Awareness Programme have been in progress to create necessary cyber security awareness through formal and informal programmes. Cyber security training facilities have been set up to provide training to law enforcement agencies and facilitating cyber-crime investigation.

4.0 Cyber security – Challenges

The Cyber space is borderless and actions in the cyber space can be anonymous. These features are being exploited by adversaries for perpetration of crime in the cyber space. The scale and sophistication of the crimes committed in the cyber space is continually increasing thereby affecting the citizens, business and Government. As the quantity and value of electronic information have increased, so to have the business models and efforts of criminals and other adversaries who have embraced the cyber space as a more convenient and profitable way of carrying out their activities anonymously.

Today adversaries are producing, selling and distributing malicious code with ease, maximizing their gains and exploiting the fact that attribution is a challenge. Malware is getting stealthier, more targeted, multi-faceted and extremely difficult to analyse and defeat even by the experts in the security field. Organized crime is fast growing and targeting the exponential growth of on line identities and financial transactions. There is increasing evidence of espionage, targeted attacks and lack of traceability in the cyber world as state and non-state actors are compromising, stealing, changing or destroying information and therefore potentially causing risk to national security, economic growth, public safety and competitiveness.

5.0 Cyber Security - Strategic Approach for XII Plan

Cyber Security requirements are quite dynamic that change with the threat environment. Threat landscape needs to be updated regularly to prevent emerging attacks. Collaboration among various agencies is needed to share information regarding emerging threats and vulnerabilities, which would help in effective protection and prevention of cyber-attacks.

It is necessary to take a holistic approach to secure Indian Cyber Space. While the cyber security initiatives of the XI plan period will be continued and strengthened, new initiatives will be put in place consistent with emerging threats and evolving technology scenario. The following Cyber Security strategies are proposed to be adopted during the XII Five Year Plan:

- Enhancing the understanding with respect to factors such as dynamically changing threat landscape, technical complexity of cyber space and availability of skilled resources in the area of cyber security.

- Focus on proactive and collaborative actions in Public-Private Partnership aimed at security incidents prevention, prediction, response and recovery actions and security assurance.

- Enhancing awareness and upgrading the skills, capabilities and infrastructure to protect the country's cyber space, to provide rapid response to cyber-attacks, to minimize damage and recovery time and to reduce national vulnerabilities to cyber-attacks.

- Improving interaction and engagement with various key stakeholders such as Govt. and critical sector organizations, sectoral CERTs, International CERTs, service providers including ISPs, product and security vendors, security and law enforcement agencies, academia, and media, NGOs and cyber user community.

- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organizations to resist cyber-attacks and improve the security posture.

- Supporting and facilitating basic research, technology demonstration, proof of concept and test bed projects in thrust areas of cyber security through sponsored projects at recognized R&D institutions.

6.0 Key Priorities and Target Deliverables for XII Plan

The cyber security initiatives will be implemented with the following six focus areas during the XII plan period:

(a) Enabling Legal Framework,

(b) Security Policy, Compliance and Assurance,

(c) Security R&D

(d) Security Incident – Early Warning and Response, Security awareness, skill development and training

(e) Collaboration

The proposed key priorities for implementation and target deliverables in respect of each of the focus areas are given below:

6.1 Enabling Legal Framework

Key Priority

The key priority of this initiative will be up gradation /development of a robust and dynamic legal framework to enable cyber security and address newer cyber-crimes.

Target deliverables

It is important to undertake research projects on the theme of cyber laws and related components like, e-commerce, encryption, IPR issues, privacy etc. Further, it is necessary that a data bank/repository of legal cases be created having details of cyber law cases decided in India. Such research projects would help in creating better legal framework and understanding about the issues related to cyber laws including cyber security.

There is a need to devise policy and procedure for obtaining authentic data stored and hosted by Indian companies on servers abroad for lawful access purpose. An encryption/decryption framework is also required keeping in view the concerns of both industry and Law Enforcement Agencies.

As the digital world is much more complex, there is a need to train judiciary, law enforcement agencies and legal practitioners about the cyber crimes, collection of digital evidences and cyber forensics.

With the ever-growing reliance on technology and spurt in newer forms of cyber crimes, it becomes imperative to introduce courses on cyber law.

In line with the requirements, the target deliverables include:

- Suitable amendments to existing legal framework
- Strengthening enforcement mechanism
- Capacity building for judiciary, law enforcement agencies, legal practitioners and students

6.2 Security Policy, Compliance and Assurance

Key priority

Cyber security policy compliance and assurance initiative needs to focus on creating an enabling mechanism for achieving conformance with provisions of IT Act, statutes and other policy initiatives of the Government and regulatory bodies.

Target deliverables

With the growing use of IT, there is an increasing need to generate and sustain user's confidence in the IT systems and transactions. Accordingly, simultaneous efforts are needed on the part of Govt., business and industry in terms of enabling frameworks, mechanisms for compliance and assurance. On its part, the Government is making efforts to identify the core services that need to be protected from cyber-attacks and is seeking to work with organizations responsible for these systems so that their services are secured in a way that is proportional to the threat perception. Industry and critical infrastructure organizations have started to focus on their ability to gain users confidence through improved software development, security engineering practices and the adoption of strengthened security models and best practices.

Most often, users of IT products depend on inputs from others to know about the security of the product. There is a need to have a mechanism to certify IT products to provide assurance from security point of view. This in turn requires creation of standards for conformance, establishment of acceptable evaluation method and process to certify products and at the same time ensure that privacy is maintained as per the prevailing regulations. This is required both for proprietary and open source products.

With India emerging as a leading outsourcing partner, there is a need to address compliance requirements to international standards and best practices on security and privacy. As such, there is a requirement for a comprehensive assurance framework that enables compliance within the country and provides assurance on compliance to out sourcing organizations and rest of the world.

The target deliverables include:

- Annual cyber security studies and surveys related to compliance and assurance
- Enhancement of crisis management plan and emergency preparedness
- Enhancement of security audit, assessment and certification infrastructure (Third party certification, Self-certification, empanelment and ratings of auditors, technical security testing, cyber security drills),
- Mechanism for generating a national cyber security index leading to national risk management framework
- Enhancement of IT product technical security assurance mechanism (Common Criteria security test/evaluation & Crypto Module Validation Program)

6.3 Cyber Security Research & Development

Key priority

The key priority of this initiative will be to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialisation leading to widespread deployment.

Target deliverables

Indigenous R&D efforts are essential for facilitating the creation of a sound S&T environment. Resources like skilled manpower and infrastructure created through pre-competitive public funded projects provide much needed inputs to entrepreneurs to be globally competitive through further R&D. Indigenous R&D efforts will contribute to creation of knowledge and expertise to face new and emerging security challenges and to produce cost-effective, tailor-made indigenous security solutions. Indigenous efforts are also required to develop products which are not available from outside sources due to export restrictions.

Viable industry-academic/R&D interactions are vital for implementation of the activities. Joint R&D programme in specific identified projects in Public Private Partnership mode will need to be explored. These joint projects are expected to speed up the development efforts and make available outcome from such joint projects for commercial exploitation and deployment in relatively short period of time. This joint R&D programme also will help in harnessing the technical skills and capabilities of institutions and organisations in public and private sector.

The target deliverables include:

- Setting up of Centres of excellence in Cryptography, Malware Research, Mobile Security and Cyber Forensics
- Creation of Centre for technology transfer and facilitating prototype to production of products
- Programs to focus on cryptography, cryptanalysis, algorithm design/ development/ hardware realisation
- Attack detection, protection, response, recovery and prevention systems
- Security solutions for cloud environment
- Mobile security solutions
- Embedded systems security particularly addressing security requirements in SCADA systems
- Cyber security assurance framework for Govt. sector

6.4 Security Incident - Early Warning and Response

Key priority

The key priority is strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange to all desired elements that are critical for cyber security, to reduce the risk of cyber threat and resultant effects.

Target deliverables

Information systems must be able to operate while under attack and also have the resilience to restore full operations in their wake. Towards this end, rapid identification, information exchange, and remediation are necessary to contain a security incident and mitigate the damage caused by malicious cyberspace activity. With the active involvement of critical infrastructure organizations, public and private institutions, a National Cyber Alert System can perform requisite analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

ERT-In is operational and is catering to the security needs of Indian Cyber community. In line with the emerging requirements, there is a need to further augment the facilities at CERT-In in terms of manpower, communication systems, tools, etc. for vulnerability prediction, analysis and mitigation, cyber forensics analysis, cyber space monitoring/ interception and critical information infrastructure security. For an effective National Cyber Security Alert System, there is a need to create/upgrade sectorial CERTs to cater to the very specific domain needs of different sectors.

Strengthening of Government Cyber Security infrastructure

The Government agencies need to set an example in the development and use of secure computer and communication networks. There is a need for priority action to strengthen the security of the Government IT infrastructure to facilitate faster and efficient information flow between various user agencies within the Government as well as effective interface with users outside the Government. In order to meet the upcoming challenges in securing the Government IT infrastructure, adequate attention should be paid to the use of appropriate technology and applications and development of suitable information security policies and guidelines.

The target deliverables include:

- Establishment of Threat, Vulnerability and Malware Research Centre
- Expansion of CERT-In Operations
- Building sensor/honeypot networks at key ICT installations

- Creation of a central knowledge repository
- Incident and response mechanism at national gateways
- Security Information Sharing and Analysis Centres (ISACs)

Cyber Security Operational Centre (CSOC) which will have co-ordination role with necessary authority and accountability in respect of cyber security defense measures

- Establishment of Regional level Cyber Security Help Desks
- Establishment of Botnet Cleaning Centres in the Govt., critical infrastructure and public sector organizations.

6.5 Security Awareness, Skill Development and Training

Key priority

The key priority is to establish cyber security capacity building and training mechanisms for developing a strong and dynamic cyber security skilled work force and a cyber vigilant society.

Target deliverables

Building appropriate human resources is vital to address upcoming security challenges and threats. There is a need to have trained manpower at different levels both in the Government and private sector. It would also be important to create interest among good IT students by creating opportunities for them. Also those who are already on the job need to be retrained and their skills upgraded. There is a need to include cyber security curriculum both at school and college levels.

Mass awareness campaign is important to create cyber security awareness among citizens. The promotion and publicity campaign could include (a) Seminars, exhibitions, contests etc., (b) Radio and TV programmes, (c) Videos on specific topics, (d) Web casts, Podcasts, (e) Leaflets and Posters and (f) Suggestion and Award Schemes.

The local law enforcement agencies at the operational level as well as central law enforcement agencies are required to be equipped to deal with cyber-crimes. There is a need for creating awareness and impart training to law enforcement agencies and judiciary regarding IT Act provisions, cyber security aspects, cyber-crime investigation procedures and cyber forensics. A separate Centre of Excellence may need to be created for this purpose. Indigenous certification programmes need to be evolved to enable affordable certification and generating certified cyber security manpower.

The target deliverables include:

- Launch of Security Education, Skill Building and Awareness Programme
- Sustained awareness campaign through electronic media

- Establishment of Cyber Security Training Labs/facilities across the country
- Establishment of examination, accreditation & certification infrastructure
- Establishment of Cyber Security Concept Labs, Digital Cyber Forensic Training Labs, Cyber Security Auditing of Assurance Labs, SCADA/embedded security labs
- Establishment of Centre of Excellence for capacity building for Law Enforcement Agencies and Judiciary

6.6 Collaboration

Key priority

The key priority is to promote shared understanding and leverage relationships for furthering the cause of security of cyber space.

Target Deliverables

The cyber threat sources and attacks span across countries. As such there is a need to enhance global cooperation among security agencies, CERTs and Law Enforcement agencies of various countries to effectively mitigate cyber threats. Accordingly, it is vital to have well-developed Cyber Security collaborative framework established through different government agencies in broad collaboration with private sector, partners and stakeholders in academia, national and international agencies. In this context, DIT should coordinate and be a focal point for all cyber security matters including critical sector in the civilian sector for effective collaboration and interface for cyber security aspects.

Target deliverables include :

- Security cooperation arrangements with overseas CERTs and industry
- Proactive engagement at UN and Asia-Pacific level
- Enhanced information sharing mechanism within the country
- Focused and sustained engagement program for law enforcement agencies and judiciary
- Creation of a tiered structure for information sharing
- Establishment of a think tank for cyber security policy inputs, discussion and deliberations

7.0 Implementation Plan

The activities to be carried out during the course of implementation of XII plan under each of the six focus areas are indicated in the following paragraphs.

7.1 Enabling Legal Framework

Studies will need to be carried out to understand the impact of new technology, crime trends and current policies on the business environment, public safety, national security and global competitiveness. Studies are also necessary on international cyber laws to harmonise Indian cyber laws with laws prevailing internationally. Based on the studies carried out, amendments required in the existing legal framework will have to be identified and appropriate means devised to strengthen the enforcement mechanism. Policies and procedures will have to be framed based on appropriate public inputs and debates. An enabling legal framework will require:

- Policy and framework to establish data sovereignty, ownership and control
- Legal framework for encryption in the backdrop of cyber security, privacy and national security
- Framework for lawful access in India with defined checks and balances and redressal mechanism
- Legal framework for usage of surveillance technologies for public safety
- Framework to protect privacy of online users
- Enabling mechanism / framework for cyber security assistance to law enforcement agencies (to take care of costs of additional equipment needed for lawful access).

Activities to create awareness about the role of CERT-In, Adjudicating Officers & Cyber Appellate Tribunal as an Authority under the Information Technology Act, 2000 will need to be undertaken. Efforts will have to be made to set standards for forensic tools and procedures in India.

7.2 Security Policy, Compliance and Assurance

The activities needed to be pursued include

- Development of crypto module validation program and operationalisation,
- Enhancement of technical capability of Common Criteria Test lab in emerging technology,
- Implementation of IT product technical security assurance program and operationalisation,
- Updation of crisis management plan,
- Enablement of development and implementation of sectoral crisis management plans,

- Carrying out periodic cyber security mock drills to assess the preparedness of critical sector organizations to resist cyber-attacks,
- Establishing institutional platform for security professionals in the country,
- Publishing guidelines and mandate for secure development and deployment of ICT systems,
- Creating a mechanism for interface between the government and public on policy compliance and assurance like interactive portal, website, etc., and
- Establishing a mechanism for incentivising security compliance and assurance.

7.3 Cyber Security R&D

The R&D Programs undertaken have to address all aspects of development: Study of the security properties of existing major systems and components, development of prototypes in selected application and infrastructure domains and simulation environments, development of deployable systems, testing of the systems developed and deployment and maintenance of trustworthy systems throughout the life cycle.

An indicative list of areas of R&D is given below:

- Indigenous cryptographic algorithms, protocols and systems for securing data at storage and transmission
- Quantum Cryptography Research
- Secure software engineering and development
- Trusted/trustworthy systems development with end-to-end security
- Tamper resistant and self healing systems
- Static and dynamic roots of trust for secure transactions
- Device security
- System-on-chip security
- Predicting future resilience of systems
- Solutions for ensuring trust of electronic transactions
- Video analytics
- Analysis and certification of commercial IT Systems
- Software assurance, code testing and analysis
- Threat Management systems
    - Active devices with built-in capability for event based monitoring
- Network penetration and vulnerability assessment tools
- Interception of encrypted communication
- Development of national security index leading to national risk management

framework

- Development of compliance and self-assessment tools, validation and implementation.

7.4 Security Incident - Early Warning and Response

The activities needed to be pursued under this initiative include

- Augmenting operating capabilities of CERT-In to address rising scale and scope of national security incident response management,
- Adopting and deploying state-of-art tools and techniques,
- Creating a structured knowledge repository with continuous streaming of information,
- Strengthening partnership and cooperation with security technology industry, international CERTs and security forums,
- Acquisition of intelligence about vulnerabilities, threats, and security risks collated from a comprehensive list of sources,
- Building of framework for engaging external expertise,
- Establishing a mechanism for technical security posture measurement,
- Establishing Security knowledge management delivery mechanism, and
- Establishing a collaboration platform for engaging with security community.

7.5 Security Awareness, Skill Development and Training

The activities needed to be undertaken under this initiative include

- Building capacity through various training delivery modes and certifications in network security, forensics, audit, security management and application security,
- Mandating Certification for security roles including CISO/CSO and those involved with critical information infrastructure,
- Enhancing Cyber Security Training and Awareness Programmes in different States across the country,
- Conducting Security Training and courses in Public Private Partnership mode,
- Conducting, supporting and enabling Cyber Security Workshops/Seminars and Certifications,
- Conducting security awareness programmes at schools level with suitable cyber security curriculum,
- Introducing specific and specialized courses in University, Engineering colleges and management institutions,
- Promoting Secure Coding Practices,

- Creating and updating role relevant standardised courseware contents,
- Establishing Centre of Excellence for capacity development of judiciary and law enforcement agencies, and
- Development of courseware on cyber law and cybercrime investigation and implementation.

7.6 Collaboration

The activities necessary under this initiative will include

- Developing bilateral and multi-lateral relationships in the area of cyber security with other countries,
- Creating models for collaborations and engagement with all relevant stakeholders,
- Enabling private-to-private and private-to-government collaboration and cooperation in the area of cyber security for sharing information on practices and breaches,
- Actively contributing to the development of international standards,
- Collaboratively conducting cyber drills and actively participating in international exercises including promoting global priority group,
- Engaging in defining controls for managing supply chain risks,
- Collaborating for bot-net takedowns and increasing consumer trust in ICT, and
- Seeking international legal cooperation by entering into bilateral/multilateral Protocols or Conventions on Cyber Crimes and Cyber Security.

8.0 Institutional arrangement and role of DIT

DIT will act as a nodal agency to implement the cyber security activities planned for the XII Plan. It will provide funding support to the programs for execution by partner agencies. Public private partnership (PPP) arrangement will need to be explored in the relevant areas like joint funding of select R&D projects, organizing awareness and training programs jointly with industry associations, state governments etc.

9.0 Summary of Recommendations

The primary objectives identified in the XI Plan for securing country's cyber space, viz. preventing cyber-attacks, reducing national vulnerability to cyber-attacks, reducing national vulnerability to cyber-attacks, and minimizing damage and recovery time from cyber-attacks, continue to be valid for the XII plan period. Accordingly, the cyber security focus areas in the XII plan period will be (a) Enabling Legal Framework, (b) Security Policy, Compliance and Assurance, (c) Security R&D, (d) Security Incident – Early Warning and Response, (e) Security awareness, skill development and training, and (f) Collaboration.

New initiatives recommended to be taken up in the XII Plan include:

- Seamless integration of agencies involved in the area of cyber security
- Creating Centres of Excellence for research in identified areas of advanced security.
- Setting up security threats, vulnerability and malware analysis facility.
- Setting up a mechanism to certify IT products to provide security assurance (including creation of standards, establishment of evaluation methods and processes and facility to certify products).
- Establishing Security Information Sharing and Analysis Centres (ISACs) across the regions and sectors for government-to-private and private-to-private information sharing.
- Establishing Sectoral CERTs.
- Strengthening infrastructure and activities at CERT-In.
- Strengthening National Cyber Alert System for rapid identification and response to security incidents and information exchange.
- Setting up Cyber Security Help Desks at regional levels for general users to provide first level of guidance and support.
- Setting up Botnet Cleaning Centres in the Government, Public, and Critical Infrastructure Sectors.
- Establishing Cyber Security Training Labs/facilities across the country in collaboration with State Governments and Private Sector

Some of the major targets/deliverables in the identified focus areas of the XII Plan are as follows:

- **Enabling Legal Framework -** Setting up of think tanks in Public-Private mode to identify gaps in the existing policy and frameworks and take action to address them. This includes addressing privacy concerns of on-line users.

- **Security Policy, Compliance and Assurance-** Enhancement of IT product security assurance mechanism (Common Criteria security test/evaluation, ISO 15408 & Crypto Module Validation Program), establishing a mechanism for national cyber security index leading to national risk management framework.

- **Security R&D** - Creation of Centres of Excellence in identified areas of advanced Cyber Security R&D and Centre for Technology Transfer to facilitate transition of R&D prototypes to production, supporting R&D projects in thrust areas.

- **Security Incident - Early Warning and Response-** Comprehensive threat assessment and attack mitigation by means of net traffic analysis and deployment of honey pots, development of vulnerability database.

- **Security awareness, skill development and training -** Launching formal Security Education, Skill Building and Awareness Programmes.

- **Collaboration -** Establishing a collaborative platform/ think-tank for cyber security policy inputs, discussion and deliberations, operationalisation of security cooperation arrangements with overseas CERTs and industry, and seeking legal cooperation of international agencies on cyber-crimes and cyber security.

Annexure 3- Smart City Guidelines for ensuring Universal Access IT Systems to empower citizens with disability to access ICT systems with ease

S. No.	Parameter	Minimum Specifications
1.	Text Alternatives	
2.	Non-text Content	
3.	Time-based Media	Provide alternatives for time-based media.
4.	Audio Description or Media Alternative (Prerecorded)	A descriptive text transcript OR audio description audio track is provided for non-live, web-based video
5.	Adaptable	Create content that can be presented in different ways (for example simpler layout) without losing information or structure.
6.	Info and Relationships	Semantic markup is used to designate headings (<h1>), lists (<ul>, <ol>, and <dl>), emphasized or special text (<strong>, <code>, <abbr>, <blockquote>, for example), etc. Semantic markup is used appropriately. Tables are used for tabular data. Where necessary, data cells are associated with their headers. Data table captions and summaries are used where appropriate. Text labels are associated with form input elements. Related form elements are grouped with field set/legend.
7.	Meaningful Sequence	The reading and navigation order (determined by code order) is logical and intuitive.
8.	Use of Color	Color is not used as the sole method of conveying content or distinguishing visual elements. Color alone is not used to distinguish links from surrounding text unless the luminance contrast between the link and the surrounding text is at least 3:1 and an additional differentiation (e.g., it becomes underlined) is provided when the link is hovered over or receives focus.
9.	Audio Control	A mechanism is provided to stop, pause, mute, or adjust volume for audio that automatically plays on a page for more than 3 seconds.
10.	Resize text	The page is readable and functional when the text size is doubled.
11.	Images of Text	If the same visual presentation can be made using text alone, an image is not used to present that text.
12.	Keyboard Accessible	Make all functionality available from a keyboard.
13.	Keyboard	All page functionality is available using the keyboard, unless the functionality cannot be accomplished in any known way using a keyboard (e.g., free hand drawing). Page-specified shortcut keys and access keys

S. No.	Parameter	Minimum Specifications
		(access key should typically be avoided) do not conflict with existing browser and screen reader shortcuts.
14.	No Keyboard Trap	Keyboard focus is never locked or trapped at one particular page element. The user can navigate to and from all navigable page elements using only a keyboard.
15.	Pause, Stop, Hide	Automatically moving, blinking, or scrolling content that lasts longer than 5 seconds can be paused, stopped, or hidden by the user. Moving, blinking, or scrolling can be used to draw attention to or highlight content as long as it lasts less than 5 seconds. Automatically updating content (e.g., automatically redirecting or refreshing a page, a news ticker, AJAX updated field, a notification alert, etc.) can be paused, stopped, or hidden by the user or the user can manually control the timing of the updates.
16.	Seizures	Do not design content in a way that is known to cause seizures.
17.	Three Flashes or Below Threshold	No page content flashes more than 3 times per second.
18.	Navigable	Provide ways to help users navigate, find content, and determine where they are
19.	Bypass Blocks	A link is provided to skip navigation and other page elements that are repeated across web pages. If a page has a proper heading structure, this may be considered a sufficient technique instead of a "Skip to main content" link. Note that navigating by headings is not yet supported in all browsers. If a page uses frames and the frames are appropriately titled, this is a sufficient technique for bypassing individual frames.
20.	Page Titled	The web page has a descriptive and informative page title.
21.	Focus Order	The navigation order of links, form elements, etc. is logical and intuitive.
22.	Headings and Labels	Page headings and labels for form and interactive controls are informative. Avoid duplicating heading (e.g., "More Details") or label text (e.g., "First Name") unless the structure provides adequate differentiation between them.
23.	Focus Visible	It is visually apparent which page element has the current keyboard focus (i.e., as you tab through the page, you can see where you are).
24.	Readable	Make text content readable and understandable
25.	Language of Page	The language of the page is identified using the HTML lang attribute
26.	Language of Parts	The language of page content that is in a different language is identified using the lang attribute.
27.	Predictable	Make Web pages appear and operate in predictable ways.

S. No.	Parameter	Minimum Specifications
28.	On Input	When a user inputs information or interacts with a control, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user unless the user is informed of the change ahead of time.
29.	Compatible	Maximize compatibility with current and future user agents, including assistive technologies.
30.	Parsing	Significant HTML/XHTML validation/parsing errors are avoided. In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features.
31.	Name, Role, Value	Markup is used in a way that facilitates accessibility. This includes following the HTML/XHTML specifications and using forms, form labels, frame titles, etc. appropriately. For all user interface components, the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.
32.	Audio-only and Video-only (Prerecorded)	A descriptive text transcript (including all relevant visual and auditory clues and indicators) is provided for non-live, web-based audio (audio podcasts, MP3 files, etc.). A text or audio description is provided for non-live, web-based video-only (e.g., video that has no audio track).
33.	Captions (Prerecorded)	Synchronized captions are provided for non-live, web-based video (YouTube videos, etc.)
34.	Captions (Live)	Synchronized captions are provided for all live multimedia that contains audio (audio-only broadcasts, web casts, video conferences, Flash animations, etc.)
35.	Audio Description (Prerecorded)	Audio descriptions are provided for all video content NOTE: Only required if the video conveys content visually that is not available in the default audio track.
36.	Sensory Characteristics	Instructions do not rely upon shape, size, or visual location (e.g., "Click the square icon to continue" or "Instructions are in the right-hand column"). Instructions do not rely upon sound (e.g., "A beeping sound indicates you may continue.").
37.	Distinguishable	Make it easier for users to see and hear content including separating foreground from background.
38.	Contrast (Minimum)	Text and images of text have a contrast ratio of at least 4.5:1. Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) bold has a contrast ratio of at least 3:1.
39.	Enough Time	Provide users enough time to read and use content.

S. No.	Parameter	Minimum Specifications
40.	Timing Adjustable	If a page or application has a time limit, the user is given options to turn off, adjust, or extend that time limit. This is not a requirement for real-time events (e.g., an auction), where the time limit is absolutely required, or if the time limit is longer than 20 hours.
41.	Link Purpose (In Context)	The purpose of each link (or form image button or image map hotspot) can be determined from the link text alone, or from the link text and its context (e.g., surrounding paragraph, list item, table cell, or table headers). Links (or form image buttons) with the same text that go to different locations are readily distinguishable.
42.	Multiple Ways	Multiple ways are available to find other web pages on the site - at least two of: a list of related pages, table of contents, site map, site search, or list of all available web pages.
43.	On Focus	When a page element receives focus, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user.
44.	Consistent Navigation	Navigation links that are repeated on web pages do not change order when navigating through the site.
45.	Consistent Identification	Elements that have the same functionality across multiple web pages are consistently identified. For example, a search box at the top of the site should always be labeled the same way.
46.	Input Assistance	Help users avoid and correct mistakes.
47.	Error Identification	Required form elements or form elements that require a specific format, value, or length provide this information within the element's label. If utilized, form validation errors are presented in an efficient, intuitive, and accessible manner. The error is clearly identified, quick access to the problematic element is provided, and user is allowed to easily fix the error and resubmit the form.
48.	Labels or Instructions	Sufficient labels, cues, and instructions for required interactive elements are provided via instructions, examples, properly positioned form labels, and/or field sets/legends.
49.	Error Suggestion	If an input error is detected (via client-side or server-side validation), provide suggestions for fixing the input in a timely and accessible manner.
50.	Error Prevention (Legal, Financial, Data)	If the user can change or delete legal, financial, or test data, the changes/deletions can be reversed, verified, or confirmed.
51.	Visual Captcha	Alternative mode of authentication should be offered to in order to be authenticated

Annexure-4: Minutes of Meeting

A discussion meeting was held in PMIDC, Chandigarh on June 9, 2018 on the Draft DPR. The minutes are listed below with their incorporation details. The same was discussed with ADC, LMC and EE, LMC for acceptance.

Category	S. No.	Observations	Our Consideration	Remarks
Video Wall Display	1	The size of display should be changed to 50" and DLP LED Screen to be used in place of LED screen	Incorporated on page no Page no 93 section 10.1 (Technical specification for Video Wall)	Cost of DLP LED display is INR X lakhs per unit. Earlier cost considered for LED display was INR X lakhs per unit.
Camera	2	Video compression in Indoor and Outdoor cameras should be H.265 or equivalent	Incorporated on Page no 112 under section 10.10 (Fixed dome camera) Page no 128 and 129 under section 10.13 (PTZ outdoor/ Box/ Bullet Camera)	
	3	Increase the Wide Dynamic Range in Indoor and Outdoor camera should to 120 db from 80 db	Incorporated on Page no 112 under section 10.10 (Fixed dome camera) Page no 128 and 129 under section 10.13 (PTZ/Box/Bullet camera outdoor)	
	4	Lens in Indoor and Outdoor camera should be P-IRIS instead of Auto- IRIS	Incorporated on Page 112 under section 10.10 (Fixed Dome Camera) Page no 128 and 129 under section 10.13 (Box/ Bullet camera outdoor)	

Category	S. No.	Observations	Our Consideration	Remarks
	5	The protocol for Indoor and outdoor camera should be Profile S & preferably G	Incorporated on Page no 112 under section 10.10 (Fixed dome camera) Page no 129 under section 10.13 (PTZ camera outdoor) Page no 130 under section 10.13 (Box/ Bullet camera outdoor)	
	6	The Casing for Outdoor and Indoor Camera should include IK 10 standard	Incorporated on Page no 113 under section 10.10 (Fixed dome camera) Page no 129 under section 10.13 (PTZ camera outdoor) Page no 130 under section 10.13 (Box/ Bullet camera outdoor)	
VMS	7	Channel Cost for VMS system is taken as lumpsum INR xx Lakhs. Include the channel cost per camera	Incorporated on page 155 under Table XVI (Field components)	INR xx channel cost per camera included for 300 camera
PoE switch	8	Include PoE + switch and suggest rationalization of PoE/ PoE + switch distribution	Incorporated on Page no 139 under section 10.13 (Industrial Grade 8 Port PoE + Switch)	8 port PoE+ switch is considered for PTZ camera where power requirement is around 25 w. Remaining Box/ Bullet/ Dome cameras will require standard 8 port PoE switch with 15 w power output. 13 units for 8 port PoE+ switch and 90 units for 8 port PoE switch
	9	Operating temperature for PoE switch should be up to 70 Degree Celsius		
UPS	10	The battery backup for Online UPS should be considered for 1 hour	Incorporated on Page no 111 under section 10.9 (UPS for CCC) Page no 140 under section 10.13 (Online	

Category	S. No.	Observations	Our Consideration	Remarks
			components for field components)	
	11	Replace SMF battery with VRLA battery	Incorporated on Page no 111 under section 10.9 (UPS for CCC with 1 hour backup) Page no 141 under section 10.13 (Online components for field components)	
Environmental sensor	12	Reconsidering the cost of Environmental sensor basis functional/ technical specification	Cost is reconsidered as INR x.x lakhs in project costing	Cost for environmental sensor was considered INR x lakhs per unit for standard specifications. PMIDC asked to reduce the specification and hence cost. Hence, INR x lakhs per unit was for basic specifications.
Network Security	13	Remove SIEM from network security		SIEM is mentioned in Cyber security framework as mandated by MoHUA, GoI guidelines. There is no cost consideration in BOQ item cost.
Civil construction of ICCC	14	Detailed scrutiny of estimate of ICCC for civil construction to avoid replicated items	Already Incorporated on Page 63 to 67	The RFP for constructing ICCC portion in Zone D Ludhiana Municipal Corporation office has civil structure items such as Earth works, shuttering, RCC, Brickwork, cement, Plastering, flooring, fixed ceiling, Painting and finishing. However, RFP for ICCC has building utility items such as DG set, IBMS, Access control solution, Fire and smoke detection, Air conditioning, furniture and interiors. The replicated items include Gypsum board based false ceiling, Partition and distemper with painting and finishing works to be part of this RFP. These items are

Category	S. No.	Observations	Our Consideration	Remarks
				around INR x lakhs
Total Project Cost		The updated Total Project Cost is INR xx.xx Cr capex cost is INR xx.xx Cr Opex cost is INR xx.xx Cr+ Taxes is INR x.xx Cr (18% GST)	Earlier Total Project Cost was INR xx.xx Cr Capex Cost INR xx.xx Cr Opex cost INR xx.xx Cr + taxes INR x.xx Cr (18% GST)	

Annexure-5: