GREATER VISAKHAPATNAM SMART CITY CORPORATION LIMITED
VISAKHAPATNAM

Request for Proposal for Selection of System Integrator to Implement Smart City Solutions

Volume 2: Scope of Work

Contents

1. Current Situation of Visakhapatnam CCC

While all the services of Greater Visakhapatnam Municipal Corporation Limited (Authority) operated in different ICT maturity levels it was decided to centralize the services in the office premises of The Commissioner – GVMC. It was envisaged to have a single comprehensive dashboard view to facilitate/hasten problem identification & quicker decision making.

In this regard Authority had established 8-seater Command and Control Center in its main office. The Center successfully launched in July 2016, in a room of 15x15 feet size, has 8 cubical and a video wall of Television Displays in 5x2 formation.

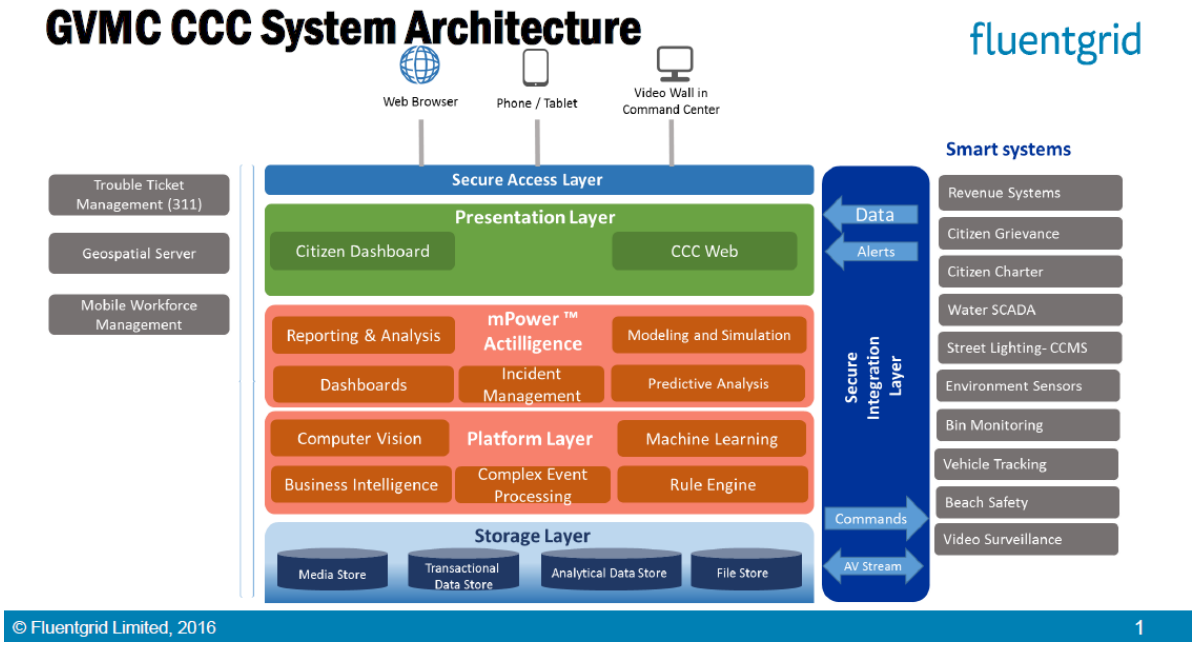
1.1. Bill of material for current CCC

The following table describes Bill of Material and brief specifications for Infrastructure for current CCC:

S.No	Item	Make, Model/ Brief Specifications	Quantity
1	TV (Video Wall)	121 cm (40 inch) Samsung TV	10 (5x2)
2	Operator Desk/Cubicals	Custom-made office cubicals (L-Shape)	8
3	Operator Desktop	Dell Optiplex 3040 desktop with 19" Display	7
4	UPS	Emerson 20 KVA UPS with battery bank for one hour	1 Set
5	Networking Equipment	Managed switch, Wireless Access point, Media Converter	1 Rack
6	Internal CCTV	Internal Analog CCTV cameras	2

Current CCC can accommodate maximum 8 operators. This is not sufficient for operating full-fledged CCC for entire city.

The systems architecture of the CCC software solution (mPower) is as follows:



1.2. Software stack at current CCC:

S. No.	Area	Software Stack	Description
1	Operating System	RHEL	64 bit version
2	SOA framework	JBoss	SOA framework from Red Hat
3	Programming Language	Java/Javabeans	Be-Spoke development
4	RDBMS	DB 2	Standard Edition
5	Web/Portal front-end	Tomcat/Apache	On RHEL

Under Corporate Social Responsibility, FluentGrid has integrated mPower to the "Data Inputs" of few utilities/e-governance service portfolios in the city of Vizag. The integration mechanism with each of these service portfolios varies depending upon the type of interface available. Below are the details for each of the integrations:

S. No.	Service Portfolio	Hosted By	Type of integration	Update Frequency	Other Details
1	Street Lights	2 separate vendors in their own data centers	REST APIs	Half Hourly	Each vendor is responsible for an area.
2	Environment Data	AP Pollution Control Board	Flat file sharing via FTP	Hourly	Data is pushed in form of flat files in the shared FTP. mPower reads the flat files. Only Air pollution data is supported
3	Solid Waste Management - Bin Monitor	Vendor	SOAP APIs	Hourly	Vendor's employees take pictures of the bin and upload. Based on these pictures the bins are approved in the vendor's

S. No.	Service Portfolio	Hosted By	Type of integration	Update Frequency	Other Details
					system. mPower pulls data from this this system
4	Solid Waste Management - Vehicle Tracking System	Vendor	SOAP APIs	-	mPower pulls data from the vendor's system
5	Beach Safety	FluentGrid	SOAP APIs	On Demand	Location of poles can be seen on GIS. Citizens can us e panic button on the poles to talk to command center operator. Operator can raise alarm by activating siren or beacon on the poles
6	Surveillance Cameras	StamPower	RTSP Protocol	On Demand (Live feed only)	Feed of 150 cameras can be seen in mPower inside the VPN
7	Water SCADA	Vendor	REST APIs	Hourly	
8	Revenue Dashboard	Authority	SOAP APIs	Hourly	SOAP based integration is done with 2 separate systems – Revenue and Budget
9	Citizen Complaints	Authority	SOAP APIs	Hourly	
10	Citizen Requests	Authority	SOAP APIs	Hourly	

2. Scope of Project Work

2.1. Overview

The project scope entails design, development, installation, operation and maintenance of the following smart city components for **Pan City.**

- Command and Communications Center (CCC)
- Enterprise Resource Planning System
- Data Center and Disaster Recovery Center (Cloud based) to cater all applications, sensors and actuators
- Integration of Systems and Sensors
- Street IT infrastructure
- Citizen services
- Command & Communications Center should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Sewerage/ Drainage system, Disaster Mgmt. System etc.
- Smart Urban Infra such as Smart Poles, Bus stops, Intelligent Transport etc.

The following activities to be undertaken by the System Integrator (SI)

1. Pre-Implementation Phase
2. Implementation Phase
3. Post Implementation Phase

Pre –Implementation Phase:

- Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.
- 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 documentation

Implementation Phase:

- Helpdesk setup, physical infrastructure setup, procurement of equipment , edge devices, COTS software (if any), licenses
- IT and Non IT Infrastructure installation, development, testing and production environment setup
- Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any)
- Preparation of User Manuals , training curriculum and training materials
- Role based training(s) on the Smart City Solutions
- SoP implementation, Integration with GIS, Integration of solutions with Command and Control Centre
- Facilitating user acceptance testing and conducting the pre-launch security audit of applications
- User training and roll-out of solution
- Integration Requirements:

- Facilitate integration of the solution with existing systems such as <list of existing system
- Develop provisions for a scalable system which can integrate with more devices of the same kind (as those deployed today) and can integrate with future applications and sensors through open standards and data exchange mechanisms

Post Implementation Scope for the Operation and Maintenance Phase:

- Deploying manpower for solution maintenance and monitoring support which includes change request management, bug tracking and resolution, production support, performing version and patch updates
- Annual technical support for all hardware and software components for the O & M period.
- Preventive, repair maintenance and replacement of hardware and software components as applicable under the warranty and AMC services during the contract period
- Provide a centralized Helpdesk and Incident Management Support till the end of contractual period
- Recurring refresher trainings for the users and Change Management activities
- Conducting disaster recovery site testing through regular mock drills

Exclusions

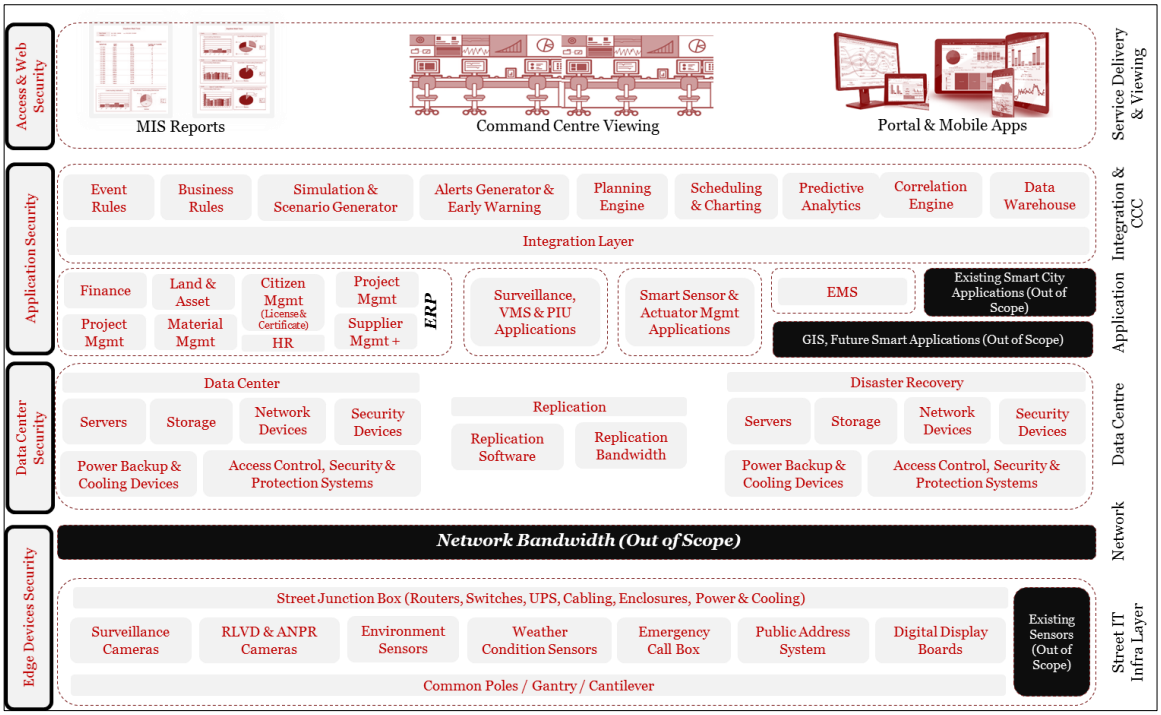
- Development of civil infrastructure for the control and communication center
- Provisioning of network bandwidth at locations requiring connectivity
- Provisioning power at locations; however, meters at all location requiring power will be provided by selected bidder

2.2. Component Architecture

Various components of the project, including expected system users, are as below and also depicted n the component architecture diagram below.

1. Street IT Infrastructure Layer
2. Network Layer
3. Data Center Layer
4. Application Layer
5. Integration Layer
6. Command and Communication Center Layer
7. Security Layer

Please note that this component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. The successful bidder shall carry out the detail requirement analysis and finalize the technical architecture in consultation with authority and its consultants. As per the figure below, the architecture of the complete network of smart elements is as follows.



- Street IT Infrastructure Layer - The sensor layer will help the city administration gather information about the ambient city conditions or capture information from the edge level devices like emergency call boxes, cameras, etc. Authority is expected to deploy multiple environmental sensors across the city, to measure ambient conditions such as light intensity, temperature, water level (for chronic flood spots), air pollution, noise pollution and humidity. The output field devices layer will contain display devices or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include digital messaging boards, environmental data displays, PA systems and emergency boxes.
- Network Layer - The secured network layer will serve as the backbone for the project and provide connectivity to gather data from sensors and communicate messages to display devices and actuators. The network bandwidth will be provided by APSFL; however, the selected bidder will have to size the bandwidth required for the overall solution, and supply and install the edge devices to utilize the network.
- Data Center Layer -The data center layer will house centralized computing power required to store, process and analyze the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. A disaster recovery site, which includes servers, storage, network equipment and security management systems will be used in case of fall back mechanism for the data center.
- Application Layer - The applications layer will include ERP modules such as finance, HR, land and asset management, citizen management, project management, material management, supplier management, etc., applications that interface and control the street infrastructure, enterprise management system to monitor and manage all IT infrastructure and street infrastructure deployed in the city, and surveillance applications.
- Integration Layer - While aspects of ambient conditions within the city will be gathered through various sensors deployed as a part of present RFP, some city specific data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the under lying architecture components and other data from system developed by government (such as police department, meteorological department, street lights department, water department, irrigation department, transport organizations within Vizag, etc.) and non-government agencies.

- Command and Communication Center Layer - The command center will enable citizens and administrators alike to get a holistic view of city conditions, and make informed decisions.
- Security Layer - As ambient conditions, actuators and display devices are now connected through a network, security of the entire system becomes of paramount significance and the system integrator will have to provide: Infrastructure security, Network security, Identity and Access Management, and Application security.

2.3. Project Implementation Timelines

The implementation timelines for the project components are as given below.

T = Date of signing of Contract Agreement
G= Go-Live Date

Phase	Command & Communication Center	ERP System	Data Center & Disaster Recovery Center	CCTV Surveillance	Environmental Sensors	Emergency Call Box	Public Address System	Digital Display Boards	Portal/ Mobile App
Project Inception Phase & Report	**T+ 15 days**								
Requirement Phase & Report	**T + 45 days**		**T + 30 days**						
Design Phase & Report	**T + 60 days**		**T + 40 days**						
Installation of HW/Infrastructure, SW Phase & Report	**T + 150 days**								
Integration Phase & Report	**T + 180 days**								
Go -Live (G) & Go-Live Report	**T + 210 days**								
Operation and Maintenance & Quarterly SLA Report	**G + 5 Years**								

3. Enterprise Resource Planning (ERP)

3.1. Salient Features of the Proposed e-Governance Application

Various features envisaged for the proposed ERP system at Authority are given below:

Architecture

- Centralized Server Architecture (n-tier architecture with web enabled user interface)
- The presentation logic should be decoupled from the business components logic
- Data access layer should be on RDBMS platform. Backend RDBMS should be of latest proven version of leading RDBMS.
- Single Database (No Heterogeneous Database to be allowed as part of the proposed solution.

User Interface

- The solution proposed should be Unicode compliant. Authority envisages requirements for both English and Telugu for Data Entry, Display, Input and Output
- Single Sign-on (for all the users) for accessing all the modules
- Any data entry needs to be carried out only once and further it should be made available as often as necessary to all the systems by providing pre-fill feature
- All modules should be homogeneous with respect to Keyboard use, screen layout and menu operations with Graphic User Interface (GUI) support
- GUI Form Administration should support
    - Changing fields or tab labels
    - Hiding fields or tabs.
    - Changing the position or size of field or labels
    - Adding restrictions like mandatory or not
    - Setting default value in a field
    - Changing list of value (LOV) contents
    - Capability to setup logic to trap conditions to pop messages in response to conditions like logical data entry errors, certain conditions etc. For an example State is Andhra Pradesh and Country is India
    - Ability to provide various configurable parameters down to the end user level so that the user screens can have different functionality for a given user.
    - Disparate information can be consolidated from a number of systems as required to produce reports and carry out ad hoc analysis and reporting

Access & Data Security

- Role based authentication for accessing various functionalities of different modules with encrypted passwords. Access Rights can be given to Individual Users or Groups
- Flexibility to define separate Role and Designation to the users. Upon transfers of officers / employees, applications / letters / complaints pending with the employee shall remain to the role and new employee will be able to take action on these applications / letters / complaints.
- User rights to various forms should be Create New Record, View existing Record or Edit existing record.
- System should be able to capture exceptions to detect frauds / mistakes

- An audit trail of changes to data in the system should be maintained to identify the users responsible for the modification. There should be a facility to create reports on audit logs
- Information Security i.e. Integrity, Confidentiality & Availability of data to be maintained

Scalability

- System should be built using Service oriented, Open Architecture
- It should be possible to add more fields to the data input screens for capturing additional business specific information without appending source code for that application/module. (for COTS modules / Bespoke development environment)
- Capability to modify existing forms to suit the requirements without requiring additional development tools
- The Application Software should have the capability to scale up to requirements for next decade like:
  - Managing the entire Property Life Cycle (Data Collaboration between various govt. departmental systems right from Land Records Department, Registration Department, Building Permission Department, Property Tax Department, Water Department, Licenses Department, Electricity Department, etc.).
  - Maintaining Information on Citizen Life Cycle (Right from Birth to Marriage, Health, Education, Driving License, Interactions with Authority (Services Availed), Death)

Citizen Interface features

- The proposed system is expected to establish an extremely efficient citizen interface. The focus has to be on maximizing the citizen convenience in availing various services of Authority and obtaining them at ease and with certainty.
- Certain design features with reference to Citizen Interface are described below:
  - Simplification of the Application Forms: Application forms for all the citizen services should be simplified and have a common design. These application forms should be available on Authority Web Portal for citizens to fill them up and submit electronically. (Reference No. needs to be issued to the citizens after submission of the filled forms online to the concerned department official for future use)
  - Multiple Channels for Service Delivery : Citizens should be able to avail various Authority services through multiple channels as listed below:
    i. Online Portal
    ii. Citizen Civic Centers
    iii. Mobile App

Integrated Application Software

- Authority intends to implement a holistic and an integrated e-Governance system. Different modules need to be seamlessly integrated with each other so that the data duplication can be avoided. This would help Authority to build a strong base for effective and efficient decision support system.

- The solution should have following functionalities: SMS Gateway Integration, Mobile device compatibility, Dashboards for Senior Management and Regular MIS Reports.
- UID integration would be one of the main focus area during implementation. It is expected that the application uses the required Gateways for UID Authentication & integration with SRDH (State Resident Data Hub).
- Authority would also develop a comprehensive GIS. It is envisaged that GIS and the proposed e-Governance systems should work in an integrated fashion to allow Authority to extract maximum benefits from the system. Bidders would have to work closely with GIS vendor to integrate GIS & eGovernance Core Application. Various indicative integration points are mentioned in the subsequent sections.
- It would be a sole responsibility of the Module owner to provide Discounting functionality to be included as part of final billing as and when required

Mobile Application

- With rapidly increasing levels of mobile penetration and continuous improvement in bandwidth, and requirements of accessibility and citizen convenience, it has been envisaged to offer more and more services over mobile devices. The SI must build strong interfaces, technologies, applications etc. for mobile devices. In order to maximize citizen convenience and bring about business process improvements, the SI must continuously innovate, upgrade and incorporate such new technologies that emerge. It is also assumed that SI would attempt to include as many services over mobile devices as possible, beyond the ones explicitly mentioned in this document.
- The mobile application must be based on latest WAP technology. A mobile application should normally be structured as a multi-layered application consisting of user experience, business, and data layers.
- All the important features and functionalities envisaged in the present RFP should be made available through the mobile application.
- The mobile application should be developed in the latest version of Android, iOS and Windows operating system
- The mobile application should be designed in such a manner that it should address the following key issues:

  i. Authentication and Authorization: Failing to authenticate in occasionally connected scenarios
  ii. Caching: Caching unnecessary data on a device that has limited resources
  iii. Communication: Failing to protect sensitive data over any carrier
  iv. Data Access: Failing to implement data-access mechanisms that work with intermittent connectivity.

- The proposed mobile application should be integrated with main core solution proposed. There should be facility to PUSH through and PULL through mechanism to get and receive information using SMS service.

Web Portal

The current website of Authority needs to be replaced to a more elaborate web portal which would facilitate the two way communication between citizens and the administrations

- The basic functionalities required for the Web portal are:
    - **Information Dissemination:** The Web portal shall provide information about Vizag City (such as history, heritage details, city guide), Details of Greater Vizag Municipal Corporation (Elected Political Members, Mayor, Municipal Commissioner of the city, Budget, Administrative Wing, Zonal Information, etc.) various Citizen Centric details/applications, grievance Redressal, Details of all Authority Officials (Emails, Employee Orders, contact information, etc.), various services provided by Authority departments, Recruitment related details, etc.
    - **Multilingual:** The portal should primarily be available in Telugu & English but as per the requirement proposed by Authority it should be available in Hindi too.
    - **Shall be available anytime, anywhere:** The portal shall be available 24 hours a day, 7 days a week, and accessible from anywhere in the world via the internet. While the technology shall be available round the clock, functional support might be available only during the normal working day- 9:30 to 6:30, 6 days a week
    - **Shall be accessible from a variety of channels:** The portal can be accessed via a variety of established channels, including individual users (through PCs, Laptops), Citizen Civic Centers, etc. Shall exchange information & services seamlessly across various departments of Authority as well as central metadata repository as specified in RFP.
    - The Web portal shall also host all the electronic forms for various services accessible to citizens from Authority. A citizen will be able to fill the form electronically (both online and offline) through internet services including Citizen Civic Centre (CCCs) outlets and submit his/her application electronically. A citizen will be able to track the status of his/her application / request at any point of time.
    - System should facilitate automatic routing of the work-items/transactions to the respective Authority department officials. Such routing of work-items/transactions should be based on the following, at a minimum:
        - Automatic allocation of work-items to the employees based on FIFO mechanism
        - The role and authorization defined in the system
        - Availability and status of employees in the system (e.g. work-items shall not be routed to employees who are on leave or whose ids are temporarily or permanently deactivated)
        - Based on the defined work-flow and the designated employees
    - Facility to define the workflow for each type of request / service.
    - Facility to capture and to provide the workflow in the CCC/Authority offices in a comprehensive manner for all the services. Both predefined and ad hoc workflows shall be provided.
    - Facility to automatically provide the status of the work item (for those work items created upon arrival of a request) through response to a request from the Citizen Civic Centers.
    - Facility to manually create a work-item (by an authorized official) and assign to an individual.

- Facility to add comments / notes / documents to a work-item during processing. It should also be possible for entering profiling information or metadata needs for a particular document (in cases where applicable) as part of this facility.
- In-built business process controls to capture the validation rules defined for processing the transactions/work-items

- Facility to register, approve or reject documents of specified type (as per applicable Acts & Bye- Laws) by an authorized official.
- Facility to view all pending transactions, retrieve the corresponding documents, print the required pages and mark the request as pending/in process/completed as per the status of the request.
- Facility for an authorized official to view pending work-items for all individuals in his/her purview.
- Facilities for an authorized official to retrieve a work-item held by an individual (in his/her purview) and reassign it to another individual.
- Facility to automatically escalate a work-item; if it is held beyond the pre-defined period by an individual. Multiple levels of escalation must be provided. Consequently, it is also necessary to provide a facility to define the threshold time limits for each transaction or service category that will be used for the purpose of escalation. This should be a parameter that can be changed by Authority from time to time.
- Access to the records / statistics should be as per the operating span/ geography of control.
- Facility to view the archived/stored documents (within the purview of the individual) along with the notes/ comments; if any.
- After successful completion of the transaction or such other processing by Authority Office staff, make the requests and associated documents as part of the electronic repository, which can be retrieved and verified at a later date.
- Facility to return the request to citizen/individual for clarifications / corrections and keep track the payment for a given period of time; so that the applicant need not be charged for resubmission of the corrected/clarified document/request.
- Facility to process complaints filed by individuals, stake holders and businesses through the work flow functions; including ability to integrate them with the compliance management, inspection, punitive and prosecution processes.
- Facility to scan documents, convert them to specified format, allow verification / authorization and upload this as part of the electronic records, with the necessary metadata into the appropriate folder hierarchy updating any necessary indices / links consistent with the application needs.
- Integrate the email / SMS functionality into the rest of the portal system such that all the escalations, request submission, routing activities are notified to the concerned users by email and SMS.
- On submission of the form appropriate message should be generated. (Reason for rejection in case of failure and acknowledgement of form submission with unique acknowledgement number in case of successful submission)
- The acknowledgement slip should be non-editable, downloadable and printable

- The portal should have the capability to integrate with payment gateways (as per RBI Guidelines on Payment Gateways) provided/supplied by System Integrator.
- The Bidder should provide 4 or more design templates for the new Web portal for Authority from which one of the design template would be selected by Authority.

❖ **Accessibility**

- Universal accessibility of the Portal through web, mobile, etc. to the entire cross-section of the target visitors including people with certain disabilities.
- Portal must be functional on as many browsers as possible without being technology or platform dependent.
- Online search result via Google or any search engine should appear first in the search results. SEO or search engine optimization is a practice to making the portal attractive to search engine.

❖ **User Management**

Web portal would be accessed by Citizens. Management of users, their access rights and verifying their credentials is critical for security and effective functioning of Web Portal. Login is the process of verifying credentials of authorized users. Password management cycle further ensures that user credentials are controlled by them and updated at regular intervals. Since other external security features such as Password key, Biometrics etc. are not feasible for all users, thus password management is an integral part of computer security procedures and provides a high degree of protection for a system. User management further helps in managing user login details and other related activities performed by them after login.

S. No.	Process Detail	Responsibility
1	Citizens would access the Web Portal. First time users would have to register themselves on the portal	Citizen
2	First time citizen users would be required to create two passwords- 1- Profile login password 2- Transaction Password	Citizen & SI/System Admin
3	All Employees of Authority would be given user id and password by System Administrator to login to the intranet portal for accessing corresponding departmental modules/applications.	SI/System Admin
4	System would prompt users to change transaction password at regular intervals e.g. every 45 days.	SI/System Admin
5	Users would also be allowed to change the password as and when required.	SI/System Admin
6	Web portal would automatically terminate the login session and log out the user in following scenarios- 1- No activity is performed by user after login for a specified time e.g. 10 minutes. 2- User accidentally closes the portal window during login session.	SI/System Admin

S. No.	Process Detail	Responsibility
7	System administrator would have all the rights to allow, deny, and provide access rights for specific information for users at his discretion.	SI/System Admin

Functional Requirement Specifications

Sr. No	Functional Requirement Specifications - Web Portal- User Management
1	System would allow user to view any Service information from Departments displayed on Web portal.
2	User – self registration and first time password change prompt. System would allow user to login and avail services from any of the modules.
3	During user id creation system would ask for Security question for any password reset request by user in future.
4	System would prompt user to create password as per security policy. Alphanumeric passwords would be asked.
5	System would ask user to create a transaction password to be used for performing any financial transaction with the concerned departments or while making any changes in the profile.
6	During user id creation, system would ask user to furnish all personal details like • Name • Sex • Age • Address • Phone no. • Email id • Occupation • Family details • PAN/License/Passport/Voter Registration No. / UID No. or any other Id proof details.
7	System would prompt user to login using user id and password created and verify them.
8	On successful password match, system would allow the user to login to the portal and allow him to access his/her profile.
9	On unsuccessful password match, System would generate password error message and ask user to enter correct password in order to login to his/her profile.
10	System would allow user to view his/her profile after login.
11	System would allow user to edit his/her personal details like Name, Address etc.
12	System would display the service related information/Instructions to fill up requested details in the entry forms like applicable fee and documents to be attached/submitted along with application request.

Sr. No	Functional Requirement Specifications - Web Portal- User Management
13	For CCC Operator, system would initially allow CCC operators to login using their login ids and passwords as given by System administrator. After first time login by all CCC operators the system would ask them to change their password (alphanumeric) as per the security policy.
14	After successfully changing the password and verifying the same on to the system, CCC operator would get access to all the modules, can accept and insert details of the requests received by the citizens for specific modules.
15	System would display instructions to CCC operators at the time of inserting details in the request form for various applications.
16	CCC Operator would read out the instructions to citizen like applicable fee, documents required along with service request and collect the same. Required documents would be scanned & attached with the request by CCC Operator.
17	System would ask CCC operator "Do you really want to submit the form" to cross-verify and register a request when he clicks on the submit button for each request.
18	System would allow Department official to login using his/her user id and password as provided by System administrator.
19	On successful password match, system would allow Department user to access requests submitted to him/her, pending for his approval or pending for field verification.
20	On unsuccessful password match, System would generate password error message and ask department user to enter correct password.
21	System would allow Department user to perform service processing functions as discussed in Department application module in following sections.
	• If any of the login details are not authenticated then the User would be shown the error message "Invalid login details. Please re-enter". • Deactivated Users should not be able to login into the application. • For all other active Users, in case of a successful login, the User would be directed to "My Dashboard/Profile" section of the application.
22	User Logout: System would allow user to log out whenever he intends to.
23	System would automatically terminate the login session if user closes the window by any chance without logging out of the system.
24	System would automatically terminate the login session if no activity is noticed in the profile after login for a specified time interval. The time period defined in "web.config" file must be configurable as per the requirements and when required. By default the time should be 15 minutes.
25	Once the user has logged out or automatically logged out by the system, the system would prompt user to re-enter User details and verify password if the user wants to login.
26	System would prompt users to change their profile & transaction password after regular time intervals.
27	System would notify the CCC/Department user on successful password change by showing alert message on screen during password change. Whereas for citizens an email would be sent to their

Sr. No	Functional Requirement Specifications - Web Portal- User Management
	registered mail id as specified in their profile informing the change in password for their user account.
28	In case user forgets the password, system would allow user to reset the password.
29	System would ask user to answer the security question created during profile creation for resetting the password.
30	System would match the user response with the user records.
31	On successful security question and answer match, system would ask user to update new password. System would prompt the user to re-enter the new password.
32	System would match the new password entered twice before submission and notify user on successful password reset activity.
33	In case of unsuccessful match, system would prompt user to enter same password twice for matching.
34	Once the password has been changed, system shall ask user to use new password for any request submission.

For any online service request citizens would fill up their details in the web page shown on screen after selecting the specific department along with attaching the required supporting documents. System would generate a receipt number for each request submitted by citizen, which would be displayed on screen after submission of the request and also the details of the request would be sent on the registered email-id of citizen. Also an intimation of acceptance of the request would be sent on his/her mobile no as an SMS. For CCC operator system would ask for all citizen details at the initial instance as mentioned in the Functional Requirement above. (Point No. 6), so the email would be sent on the citizen email id and also an intimation would be sent to citizens mobile no.

- **Reliability**
  - Disclaimers, privacy and security policies, terms and conditions and copyright information to encourage people to use e-government services and information

- **Profile Management:**
  - Enable registered users to manage their accounts and profiles and as appropriate

- **Security**
  - Based on ISO 27001/BS 7799 standards, user access to the system must be through a single sign on process, which should involve specification of a user Identification, a password and the applications displayed must be as per the user profile and authority. The system should allow user to change his/her password based on a given time frame as well as give the user the option to change his password at any time. The system should disable the User profile after five unsuccessful log-on attempts. The system should be able to log successful and failed attempts to the system.
  - This section highlights the security architecture proposed for the e-Municipality system –

A. General Requirements

i. Information, hardware and software would be secured to both internal and external parties (such as through password encryption).

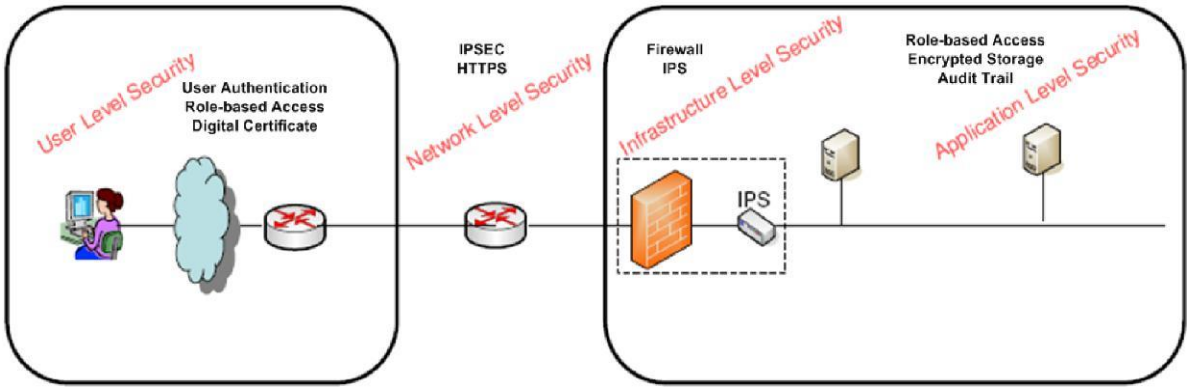
ii. The security measures adopted should be of wide range and of high quality, to create confidence in the systems security and integrity. The system should be protected against deliberate or accidental misuse that might cause a loss of confidence in it or loss or inconvenience to one or more of its users.

iii. System level and application level authentication between portal and between applications within portal, if any, to ensure against security attacks

iv. The application system would strictly be password protected and access to different modules would be role specific

v. Audit trails would be provided to allow the activities of users to be monitored.

vi. For the system, security must be available at Functional level, User group/class level, Menu level and Transaction type level. The following figure depicts the hardware level security at Data Center.



vii. There should be four levels of security considerations as described below:-

a. Key Security Considerations at the User level:
- (i) User authentication
- (ii) Role based access to services, transactions and data

b. Key Security Considerations at the Network/ Transport level:
- (i) Network Link Encryption (IPSEC)
- (ii) Encrypted HTTP session using SSL (HTTPS)

c. Key Security Consideration at the Infrastructure Level:
- (i) Firewall to filter unauthorized sessions/traffic
- (ii) Intrusion Prevention System to detect/prevent unauthorized activities/sessions

d. Key Security Considerations at the Application & Database level:
- (i) Secure storage of user credentials
- (ii) Server–to-Server communication encryption
- (iii) Secured/ encrypted storage of data/ data elements in the Database & DB Backups
- (iv) Comprehensive logging & audit trail of sessions and transactions

B. Security Requirement for Portal

This section elaborates specific security requirements which would have to be provided in the Web portal.

i. *Effective password management controls*: The portal solution would have the ability to perform password management functions including:
    a. Controlled password expirations,
    b. Forced password change with optional grace logins,
    c. Minimum password lengths (eight characters),
    d. Alphanumeric password standards,
    e. Minimum number of numeric characters,
    f. Non-dictionary words,
    g. Password history logging and user lockout from failed login attempts.

ii. *Access control to information*: The security solution would be facilitating access controls for specific users to only certain resources/services in the portal and at the same time system must provide single sign-on to all functional areas.

iii. *Scalable and portable solution*: The security solution would provide scalable access services for the Portal, including scalability in terms of number of users, user groups, resources, and access control policies.

iv. *Secure Communication over the network*: The portal should support the exchange of data through secure channels of communication protected by standards such as the SSL protocol. Such facility should provide the following functionality, at a minimum:
    a. *Confidentiality of communication*: Encryption of all messages between client and server
    b. *Authenticity:* Digital certificates to authenticate all messages between client and server, confirming the identities of messages/transactions
    c. *Integrity:* Message Authentication Codes (MACs) provide integrity protection that allows recognizing any manipulation of exchanged messages.
    d. Secure communication between the user and the portal with SSL and encrypted logon information using algorithms with strong key lengths.

v. *Uninterrupted security services /automated load balancing to backup services:* The security solution should provide for load balancing/high-availability to enable a fully scalable and available solution. It should enable continued service on failure of one or more of its component parts.

vi. *Secure storage of critical items:* The security solution would provide for the ability to securely store critical data within the LDAP or other user directory structure or any user related databases so that database administrators or any unauthorized users do not have access to items such as transaction information, passwords, user profiles and other critical items.

vii. *Detailed session management abilities*: The security solution would provide for session settings such as idle or max session time-outs, concurrent sessions and other session control settings.

viii. *Web Access Filtering*
    a. The portal security solution should examine all traffic to all resources of the solution and all access attempts to the portal or directly to any resource

managed/access by the portal, should be intercepted by the security solution, and examined for authentication and authorization requirements defined for the resource.

b. At the same time, the performance overhead of examining all web-traffic and performing the authentication and authorization requests should not become the bottleneck in the service delivery process and should not impact on the performance of the portal solution.

ix. *Security Monitoring*: The security solution implemented for portal must be capable of comprehensive logging of the transactions and access attempts to the resources/applications through the portal. It should be capable of logging transaction history, unauthorized access attempts, and attempts to login that fail. It should also be capable of notifying appropriate Authority officials of any suspicious activity.

x. *Security- User profiles*:

a. Initially the citizen would have to create his profile by Registering at the web portal by specifying the details as asked in the Registration form. Citizen also needs to create profile and transaction password at the time of registration.

b. For the first login by a user at CCC/Authority offices, the system should prompt the user to change his password.

c. When a user logs-in, the system should show him the date & time of last login

d. The System must restrict user access based on the privileges assigned to the user

e. The system should maintain a log of all the activities carried out by a user along with a date and time stamp.

f. The System must maintain a log of all activities carried out by an administrator.

xi. *Other Security Services*:

a. The sensitive and confidential information and documents of the users must be stored in an encrypted format in the database.

b. The system should support 128-bit encryption for transmission of the data over the Internet.

c. All the systems in solution network should run most up-to-date anti-virus software to avoid malicious programs to cause damage to the systems

d. Any access to the end users to database should only be via application/portal authorization

e. Physical security for the solution should address securing all information assets from physical access by unauthorized personnel. For example, the data center server infrastructure should not be physically accessible by anyone other than the persons responsible for on-site maintenance of the systems

f. The technology solution should comply with ISO27001 standards. Security certification process should include audit of network, server and application security mechanisms.

xii. *Auditing features and Requirements*: The security solution for portal must provide the capability to track and monitor successful and unsuccessful transactions with the portal. Accountability for transactions must be tied to specific users. The architecture/systems should facilitate audit of all significant security events including authentication, accessing of services and security administration. The auditing capabilities need to be built into various layers of the portal infrastructure including Application Software, Operating System, Database, Network, Firewall etc.

a. SI would have to implement Intrusion Prevention Systems (IPS) at all the critical network points, both internal and external, for monitoring and addressing the unauthorized access attempts and the malicious activities in the network.
b. Information and communications systems handling sensitive information must log all security relevant events. Examples of security relevant events include, but are not limited to:
    i. attempts to guess passwords,
    ii. attempts to use privileges that have not been authorized,
    iii. modifications to production application software,
    iv. modifications to operating systems,
    v. changes to user privileges, and
    vi. changes to logging subsystems
c. Detailed audit trail of transactions performed in the system (approvals, rejections, renewals etc.) which should capture the details of individuals performing the transactions, date & time stamp etc.
d. Stringent security measures should be implemented surrounding the audit data to ensure that audit records are not modified, deleted, etc.
e. The web portal should facilitate reporting facilities in a simple and readable manner for the Authority officials to review audit trails for the transactions occurring in the system.

xiii. *Security Requirements for Portal Databases*: Database is the critical components of the portal, which stores the entire data related to Services & functions. Following outlines the security requirements of the database, which at a minimum (included but not limited to) should be implemented.

a. The database for portal should support and implement encryption capabilities while transferring data over networks, and ability to encrypt data stored in the database at the column level
b. Comprehensive auditing for inserts/ deletes/ updates / selects to quickly spot and respond to security breaches.
c. The critical data and the related documents stored in the portal database should be stored in encrypted format.

C. Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) on application and database server can stop well-known attacks, new/ unknown attacks and encrypted-tunnel based attacks that target the application/ database servers. The following are the benefits of using IPS:

i. IPS monitors system activity and notifies administrators when it suspects suspicious activity
ii. IPS blocks suspicious executable or processes from running by default
iii. Allows System Administrators to determine which traffic and applications to permit and block
iv. Protects Files, Registry and Computer Settings of Operating System and Application Integrity Check
v. Reduces the risk of downtime caused by malware, spyware and other malicious content and helps to keep your critical application up and running
vi. Helps to log all relevant events to help with compliance, reporting and investigations.

D. Antivirus & Anti-Spam

The following activities need to be performed.

i. Monitor the Antivirus tool updated on daily basis and ensure that the latest patches are updated in all the systems.
ii. Monitor the security console and clean the virus from the systems, which are affected and if necessary, isolate those systems to avoid further spreading of viruses.
iii. Alert users on new virus breakouts based on the info received from CERT-IN
iv. Install, configure and test latest security patches.
v. Troubleshoot and rectify all virus related problems reported and also escalate if not rectified by the Antivirus tool.
vi. Monitor the client security tools and adhere to the security policies as finalized with the Authority.
vii. Monitoring the efficiency and effectiveness of the Anti-Virus tool.
viii. Registering and updating the Anti-Virus tool on the server and the clients periodically
ix. Providing feedback on any new viruses detected and alarm/alert the protection systems

- Security techniques and measures provide security measures to protect information belonging to the Portal and the entities (departments) from unauthorized access, modification, or deletion.
- Monitor, log and audit security incidents with date/time stamping.
- Maintain and ensure data integrity and visitors' confidentiality and privacy.
- Implement a password complexity, automatic blocking of user logins after given number of unsuccessful login attempts, controlled access to content stored on the portal and logging of security incidents.
- Provide a facility to securely store critical data within the transaction database so that administrators don't have access to items such as transaction information, passwords, user profiles and other critical items.
- Provide a facility to perform password management functions including: controlled password expirations, minimum password lengths, and enforcement of alphanumeric password standards, password history logging, and user lockout from failed login attempts

- Authenticity of the sender of each service request to be established by login-password as specified at the time of registration by the sender

❖ **Unified Messaging system:**

- **SMS**: The Web-Portal shall have facility to send SMS to Mobile number of a citizen which was provided while requesting certain information or service. The SMS shall be auto-generated based on the information or service requested on occurrence of its change of status. All the application needs to be integrated with SMS gateway.
- **E-mail:** The Web-Portal shall have facility to send e-mails to
  - The e-mail address of a citizen, provided while requesting certain information or service.
  - The e-mail shall be auto-generated based on the information or service requested on occurrence of its change of status.
  - Reporting Officials maintaining the hierarchy, in cases of delay (as per the Citizens' Charter) in providing services.

Workflow Management System as an Application:

Workflow Management System would serve as an integrated functionality across all the departmental modules to receive and process the request / applications received via any of the service delivery channels. Each request/application should be processed via workflow engine mechanism. I.e. each of the application should be routed to the respective department official's activity dashboard. WMS should also have a facility of delegation of powers.

.

Following functionalities should also be part of the integrated applications proposed by a successful bidder:

1) **Role based Access Management System** – Proposed User management module should have following categories of Users:

   a. Super User – IT Cell, IT Manager, Municipal Commissioner
   b. Master Admin – IT cell
   c. Admin – IT Manager, HoD of a department
   d. Regular / Anonymous Users – Employees from various departments of Authority, Citizens requesting/applying for any service/information.

   Available information and user options will vary on all pages throughout the system depending on privileges assigned to the users.

2) **Admin Section** – This section should be privilege restricted and should have the facility to:
   a. Create, modify delete Users and Groups
   b. Assign and remove privileges(modules, sub-modules, workflow & other) to individuals and groups
   c. Administer restricted sections / modules / Webpages

3) Content Management

- System Integrator would be responsible for maintaining and uploading of content on the web portal for implementation phase and also under operation and maintenance period of 5 years.

- Necessary approval from the associated department needs to be taken by the System Integrator for uploading and maintaining of CMS (Content Management System).

General

- The system requires continuous availability (24 * 7)
- The system shall be designed in such a way so as to ensure that the loss of data is minimized due to network 'drop outs'. Automatic refreshing of data at specified time intervals. The information shall be refreshed from the database and shall not require user intervention
- System should have an online help capability, which should be customizable. Should have a facility for online learning and collaboration
- All reports should be query based and should have options like departments zones, wards, employees, from date, to date, etc.
- Authority Users will access the system using Ethernet LAN / Lease Line / RF / Internet

3.2. City Civic Center Module

Functionality	Integration required with
A] Citizen Help Desk	
▪ Facility to lodge New Complaints, Check Status	CCRS
▪ Facility to check citizen data ○ Bill Dues ○ Application Status ○ Payment Status ○ Renewal Status ○ Certificates issuance	All Departmental Modules, KIOSK Module, Web Portal
▪ Citizen Charter	CCRS, HRMS
B] Application Acceptance & Delivery of Outputs	
▪ Department-wise categorization	
▪ Allow system to accept service specific inputs	
▪ Capture of Mobile No. of Applicant	
▪ Re-submission of rejected application after compliance	
▪ Check-list for documents to be submitted along-with application	
▪ Define citizen charter (list of the officers & duration for service delivery)	HRMS
▪ Fees to be accepted	Accounts
▪ Generate Token of Application acceptance	
▪ Rejection Note in case of inadequate application	
▪ Marking the application to Corresponding Department / Ward / Officer	WMS
▪ Delivery of the output through CCC / Internet / KIOSK	Departmental Modules
▪ SMS alert to applicant upon decision	SMS Gateway
C] Payment Acceptance	
▪ Property Tax	Accounts, Departmental Modules, Property Tax
▪ Water Tax	
▪ Professional Tax	
▪ Vehicle Tax	
▪ License	
▪ All Departmental Services	
▪ Tender Document Fees	
▪ Any other	
D] Citizen Services (General) [Such *services won't have any department specific functionality. CCC module, by using Workflow Management System should be able to deliver these services*]	
▪ Marriage Certificate	
▪ NOCs for other govt. departments	
▪ Booking of various Corporation premises such as Halls, Community Halls, Open air theatre, Amphitheatre, Auditorium, Ground, Party Plot, etc.	

Functionality	Integration required with
▪ Issue of health license for shop having area less than 40 sq. mt	
▪ Any other services	
E] Marriage Registration Sub-Module	
▪ Design of Forms & Database for the Marriage Registration Functionality	
▪ Capture of Thumb Impressions of the Applicants & Witnesses	
▪ Capture of the Photograph of the Applicants & Witnesses	
▪ Scrutiny of the Applications	
F] Professional Tax	
▪ Enrollment and Registry Enrollment of firms. (PEC & PRC)	Property Tax, GIS
▪ Details of firms along with their contact details, address details	Property Tax, GIS
▪ Outstanding Professional Tax details for different firms.	Property Tax, GIS
G] Vehicle Tax	
▪ Capturing Vehicle details such as Engine No. / Chassis no. , etc.	
▪ Capturing type of Vehicle for collection of taxes.	
▪ Capturing details of the Vehicle owner (Name, Address, Contact details, etc.)	
H] MIS	
▪ SMS alert to applicant upon decision	SMS Gateway
▪ Services Statistics ▪ CCC-wise / KIOSK-wise ▪ Department-wise	
▪ Officer-wise list of services pending beyond the stipulated time	HRMS, WMS
▪ Marriage Registration periodic / statistical reports	
▪ Professional Tax collection / outstanding report	
▪ Interest calculation for outstanding Professional tax	
▪ Defaulter list for Professional Tax payment	GIS
▪ Property Tax collection report	
▪ Report containing license issued details and payment collected for the same.	
▪ Vehicle Tax collection report	
I] Additional Functional Scope after validation	
▪ RTI	
▪ Issuing License ➢ Gumasta License ➢ Hawker's License ▪ Health license for shop having area less than 40 sq. mt	

Note: CCC Module should get integrated with KIOSKs setup by Authority to accept inputs & give outputs.

3.3. Document & Workflow Management System

Functionality	Integration required with
A] File Tracking System	
▪ Scanning & Marking the inward to the respective department	CCC
▪ Incorporation of separate hierarchy for RTI letter movements & Commissioner Office. ▪ Fresh applications ▪ Appeals	CCC, Web, KIOSK
▪ Tracking of the Inward	CCC
▪ File Closure to be carried out as per the final decision of respective authorities.	
B] Document Management	
▪ Storing of document (Image & Metadata)	
▪ Support for viewing a large number of file formats without the need of having the parent application. The system should support all commonly used file formats as MSOffice, Acrobat, TIF, JPEG, GIF, BMP, etc.	
▪ Association of the document with Workflow Management System	
▪ Movement of the document based on selected parameters	
▪ Provision to edit the document Metadata	
▪ Versioning of the document	
▪ Provision for marking comments	
▪ Archival of data on pre-defined parameters	
▪ Role based access to the documents	HRMS
▪ Final Decision by the Decision Authority	
C] Workflow Management System	
▪ Movement of Proposals on various parameters	Projects, Central Stores, CMSO
▪ Facility to mark the application to pre-defined hierarchy	HRMS
▪ Inbox for officers (listing applications received)	
▪ FIFO principle for taking action on application	
▪ Creation of a Note Sheet for Scanned Documents	
▪ Alerts for delay in action	
▪ Information/Alert to be sent to higher authority in case of delay in action by specific employee of the department	
▪ Pre-defined scrutiny for citizen applications	
▪ Display of all application data during scrutiny process	Accounts
▪ Check-list for rejection	
▪ Facility to mark the application to other officer	
▪ Facility to mark the application to other department for their NOC / Comments / Input	WMS
▪ Final Decision by the Decision Authority	WMS

3.4. Property Tax Department

Functionality	Integration required with
A] Capture of various details of the Property	
▪ Ward/ Zone/ Block/Route – Administration or Geographical divisions	GIS
▪ Property Holder's Name – One or multiple owners	
▪ Property Holder's Email ID / Mobile No.	
▪ Property Holder's Address (Present Address, Permanent Address)	
▪ Property Location details (FP No., TP No., Survey No., etc.)	GIS
▪ Property address	GIS
▪ Linkage with Building Permission Module to carry forward building details	
B] Capture of various details required for Property Assessment	
▪ Type and Sub Type of Property	GIS
▪ Usage of Property	GIS
▪ Construction Class / Vicinity Factor / Amenity Factor	GIS
▪ Age of Building	GIS
▪ Property tax as per rent assessment.	GIS
▪ Any other factor required for Assessment	GIS
▪ Re-Assessment of the affected properties to be carried out again in case of road widening.	GIS
C] Self-Assessment Module	
▪ Allow citizens to enter their property details through Web Portal	Web Portal, GIS
▪ Option to the citizens to submit their Assessment to the department for confirmation	GIS, WMS
D] System based calculation of Ratable Value	
▪ Room-wise / Flat-wise/ Whole Property Assessment	
E] Tax Generation	
▪ Tax Generation as per Rate Chart	
▪ Tax Exemptions	
▪ Bifurcation of rates for General Tax, Fire Fighting, Water Tax, Conservancy Tax, Educational Cess, etc.	GIS
F] Other relevant Details for Property	
▪ Property history	
▪ Advance property tax payment	
▪ Property Rental details	
▪ Date of Assessment	
G] Other Departmental Process	
▪ Generation of Special Notice	
▪ Objection	
▪ Hearing	
▪ Property Billing o Individual flat-wise billing/ Property wise billing o Calculation of Property Tax as per prevailing Stamp Duty for different areas.	Accounts

Functionality	Integration required with
○ Interest Calculation ○ Consideration of Advance paid earlier	
▪ Demand Notice Generation	
▪ Issue of Warrant Notice	
▪ Seizure of Property	
▪ Auction of Property	
▪ Rebate Calculations	Accounts
▪ Automatic mailing of Bills / Notices to the E-Mail ID	
▪ Advance / Excess Collection / Refunds	Accounts
▪ Cheque Dishonor and Outstation Cheque charges	
▪ Facility for online tracking of bounced checks	
▪ E-Mail / SMS to be sent to the owner upon transactions	SMS Gateway / Web Server
H] Citizen Services	
▪ Change in Property Ownership	Accounts
▪ Splitting of Property Tax Assessment	
▪ Duplicate Bill	
▪ Assessment Certificate	
▪ Copy of Property Tax Assessment Extract	
▪ No Dues Certificate	
▪ Payment of Property Tax	
▪ Linkage with Grievance module for Property Tax related grievances	Grievance Redressal
I] MIS	
▪ Demand / Collection Register	GIS
▪ Assessment Register	GIS
▪ Closing Register	
▪ Ward-wise / Zone-wise Recovery reports	GIS
▪ Top Defaulters Report	GIS
▪ Occupancy wise / Flat wise report	
▪ Escalation alert to be generated for new property assessments to zonal assessors, Deputy Municipal Commissioner and Municipal Commissioner.	Building Permission Module
▪ Tax-wise Recovery Details	
▪ Tax-wise Demand Details	
▪ Advance Payment Reports	
▪ Objection / Hearing Details	
▪ Inspector wise report (Assessment of property as per Building permission / Citizen request / Inspection)	
▪ Assessment as per citizen / Assessment as per inspector	
▪ MIS reports for self-assessment, concessions.	
▪ Alerts from License Module upon New License / change in business	License Module

Functionality	Integration required with
J] Other Requirements	
▪ Data Porting / Data Entry Suite	
▪ Query of Property Dues	CCC, Web Portal
▪ Scope to link up to Land Records / Registration system	

3.5. License Module (Shops / Food / Market)

Functionality	Integration required with
A] Citizen Services	
▪ Issue of New License (Food, Market, Hawkers, Gumasta, etc.)	CCC, Accounts, Property Tax, Professional Tax sub-module
▪ Duplicate License (Food, Market, Hawkers, Gumasta, etc.)	
▪ Change in Name of Business	
▪ Change in Business	
▪ Transfer of License	
▪ Renewal of License (Food, Market, Hawkers, Gumasta, etc.)	
▪ Cancellation of License (Food, Market, Hawkers, Gumasta, etc.)	
B] Issuance of License	
▪ Capture of License Details o License Holder's Details – One or multiple owners o Capture of Mobile No. / E-Mail ID o License holder's photograph(s) (optional) o Link to Property Number (optional) o License Details – Temporary/ Permanent License, Name of Business, Business Address, Business Details o Trade/ Business Details – License Type, Subtype - multiple levels to define types and sub types. o License type, sub-type, unit of measure wise license amount.	GIS, Property Tax Assessment, Professional Tax sub-module
▪ Calculation of License Fee	Accounts
▪ License Certificate	
C] Other Departmental Process	
▪ Scrutiny of Applications	WMS
▪ Inspection Entry	
▪ Generation of Show cause Notice	
▪ Hearing	
▪ Reminder Notice for Renewal	
▪ Cancellation of License/Revoke by Force	
D] MIS	
▪ License Register	
▪ List of Defaulters	GIS
▪ Reminder Notice for Renewal	
▪ Demand / Collection Register	
▪ Reports showing Changes in License Types, Business Partners, Cancellation Licenses, etc.	
▪ Facility to forecast the impact of reduction / deduction of License Fee	
▪ Reports w.r.t. Bills / Notices generated	
▪ E-Mail / SMS to be sent to the owner upon transactions	SMS Gateway / Web Server
E] Other Requirements	
▪ Data Porting / Data Entry Suite	

3.6. Building Permission Module

Functionality	Integration required with
A] Citizen Services	
▪ Layout Approval	CCC, Accounts, GIS, SMS Gateway, Property Tax, Professional Tax
▪ Building Permission / Commencement Certificate	
▪ Revised Building Permission (to be issued only after updating the same into GIS)	
▪ Renewal of Building Permission (to be issued only after updating the same into GIS)	
▪ Plinth Completion Certificate	
▪ Occupancy Certificate	
▪ Alert to be issued to all the property assessors to each of the zones.	
▪ Cancellation of License	
▪ New / Renewed License for Engineers/ Structural Engineers/ Architect/ Clerks of Works/Developers	
▪ Zone Certificate	
▪ TPI Opinion (Betterment Opinion by Zonal Office)	
▪ Transfer of Development Rights / Ownership change	
▪ Certified copy of plan	
▪ Old property data retrieval	Property Tax Module
▪ RTI – Apply online for information related to proposal	SMS Gateway, WMS
▪ Single complaint can be handled by multiple department	
▪ Online submission facility should be made available for registered Architects	GIS, Property Tax Module
▪ Supervision/Checking to be carried out for status of approved building plan by Department officials.	
▪ Fire Safety NOC	
B] Defining Charges	
▪ Development Charges	Accounts
▪ Scrutiny Charges	Accounts
▪ Other Charges	Accounts
C] Departmental Process	
▪ Scrutiny of Applications	GIS, HRMS, WMS
▪ Alerts to inter departmental Officers as per timelines of approving or rejecting proposals	
▪ Site Reports	
▪ NOCs from different departments	WMS
▪ Alert to be sent to Property Tax Department after issuance of Building permission, Plinth , Completion & Occupancy Certificate (Color code based GIS system)	Property Tax, GIS

▪ Versioning of proposal for more than one iterations	GIS
▪ Facility for query for the stage of completion to be made available	GIS
▪ Advocate dates for departmental cases	Legal, SMS Gateway
▪ Audit objection / audit para for departmental cases	Audit
▪ TDR awarded information	Land & Estate, Property Tax, GIS
D] MIS	
▪ Application Pendency Report	WMS
▪ Building Permissions / Occupancy Certificates taken for a particular period	GIS
▪ List of Building Permissions taken but Occupancy Certificate not Taken	
▪ Impact analysis for Drainage / Water based on the building permission given.	Water
▪ Revenue Related Reports (Scrutiny Charges / Development Charges)	
▪ E-Mail / SMS to be sent to the applicants	SMS Gateway / Web Server
F] Other Requirements	
▪ Data Porting / Data Entry Suite	
▪ Generation of Alerts to other departments w.r.t. infrastructure requirements, upon completion certificate	WMS, Projects, SWM, Water
G] Additional Requirements	
▪ Generate Drill Down Progress Reports	WMS
▪ Hearing of Grievance Case registered in respect to the Building permission/Building Utilization, etc.	

3.7. Water Connection Module

Functionality	Integration required with
A] Citizen Services	
▪ New water Connection	Accounts, SMS Gateway
▪ Closing of Connection (Permanent / Temporary)	
▪ Change of use	
▪ Reconnection	
▪ Issuance of Plumber license	
▪ Water testing for citizens within Authority limits	
▪ Renewal of Plumber license	
B] Defining Various Charges	
▪ Water consumption Charges for metered and non-metered connections	Accounts, SMS Gateway
▪ Water connection charges	
▪ Scrutiny Charges	
▪ Deposit for various connection size & category.	
▪ Water testing rates	
C] Departmental Process	
▪ Capture of various details of the Water Connection o Consumer Details- Property Details, Owners Details, Link to Property Number. o Metered/ Non Metered Connections o Multiple Usage type - Domestic, Commercial, etc. Tariff Category.	Property Tax, GIS
▪ Connection Details- Connection Size, Distribution Line, Pressure	GIS, Property Tax
▪ Pressure drop due to new connection on a line.	GIS
▪ Compliance for 'No dues' for property Tax	Property Tax
▪ Meter Information - Meter No. / Make / Cost	
▪ Meter Restoration Details	
▪ Scrutiny at various levels for citizen services	
▪ Road digging charges to be taken from GIS system	GIS, Accounts
▪ Work Order Printing for new connections, re-connections and closing of connections.	
▪ Meter Reading Entry o Meter Reading Data Entry o Meter Cut off- Restoration	
▪ Uploading of captured site scrutiny data into the system at department	
▪ Temporary Disconnection	SMS
▪ Bill Generation o Billing for Metered and non-metered connections o Billing schedule for different connection category o Consideration of advance paid if any o Interest calculation on arrears o Bill correction	Accounts, SMS

Functionality	Integration required with
▪ Bill Printing	
▪ Collection from CCC	Accounts
▪ Handling Cheque dishonor and outstation Cheque charges	Accounts
D] MIS	
▪ Connection Outstanding Register	
▪ Bill Acceptance Register	
▪ Meter reading report	
▪ Consumption statement	
▪ List of consumers ward, category & size wise	GIS
▪ List of connections	
▪ List of closed connections	
▪ Ward-wise / Zone-wise Recovery reports	
▪ Top Defaulters Report	
▪ Tax-wise Recovery Details	
▪ Tax-wise Demand Details	
▪ Advance Payment Reports	
▪ Bill status for bill generation	
▪ Faulty Meter Report (Based on Complaints)	CCRS
▪ Illegal connection reports (Based on complaints)	CCRS
▪ Water quality test report	
▪ Ward wise / zone wise / line water pressure report	
E] Other Requirements	
▪ Data Porting / Data Entry Suite	
▪ Query Water Dues	CCC, Web Portal
▪ Scope for integration with SCADA system (Meter Reading)	

3.8. Accounts Module

Functionality	Integration required with
A] Masters	
▪ Account Head Definition	
▪ Account Grouping and Sub-Grouping	
▪ Bank Account Details	HRMS
▪ Vendor Details	Procurement Module
B] Departmental Process	
▪ Budget Preparation, Distribution and Management System o Budget Classification o Department-wise estimated provision, revision for income and expenditure o Budget Appropriation between different budget heads through approval process o Administrative approval / dis-approval of works linked to budget availability	Procurement, Materials Management, Central Stores, CMSO, other related departments
▪ Receipts through Internet / CCCs / KIOSKs o Counter-wise Collection Detailed and Summary Reports o Revenue Stamp Management o Cheque/ Cash Deposit Slips into Bank o Capture of Cheque Dis-honor cases, Remittance entry	All Department modules
▪ Payment Management o Bill / Liability Entry o Payment Authorization o Payment Voucher (Full or Partial Amount) o Maintaining Check details, Check Printing o Recording of Check Issuance Details o Recording of Cheque Cancellation details	All Department modules
o Types of Discounts (Recommending Authority for discounts) o Amount of Discount (percentage of final bill or lump sum value)	Hospital Management System
▪ Security Deposit / Earnest Money Deposit Management / Bank Guarantee Register	
▪ Zone/Ward/CCC wise Bank Collections	
▪ Loans Management o Maintenance of Loan Details o Alerts for Loan Installment Payments o Loan Installment Payments o Generate Bill and Carry out payment o Interest Calculation	

Functionality	Integration required with
▪ Grants Management o Maintenance of Grant Details o Timing of Grant (Regular/Irregular) o Utilization Details o Interest Calculation o Utilization Certificates o Generate alerts for Grant Received or not.	
▪ Debt Management	
▪ Accrued Payment Management / Fund Management	
▪ Investment Management o Maintenance of Investment Register o Alerts on due dates o Comparison of different options for Investments o Interest Calculation o FD Register o Generate Voucher/Challan	
▪ Advance Managements	
▪ Bank Reconciliation	
▪ TDS/ VAT Register, Online Payment of Tax	Related Departments/Modules
▪ Maintenance of Bank Account wise balances	
▪ Integration of Ledger A/c with ECS Payment	
C] Reports	
▪ Cost Centered Accounting Reports	
▪ Ratio Analysis, Trend Analysis	
▪ Department-wise, Cost Center-wise Income / Expenditure reports / Account Code wise Reports	
▪ Generation of Deposit Slips	
▪ Security Deposit Register	Procurement Module
▪ Grants Register	
▪ Loans Register	
▪ Investment Register	
▪ Advance Register	
▪ Bill Register	
▪ Payment Register	Related Departments/Modules
▪ Outstanding Bill Register	
▪ Reports on Receivables	
▪ Reports on Payables	
▪ Cash Book (Detailed & Summary)	
▪ Function-wise Expense Subsidiary Ledger	
▪ Journal Book	
▪ Ledger Book	

Functionality	Integration required with
▪ Cheque Issue Register	
▪ Trial Balance, Income & Expenditure Statement	
▪ Balance Sheet	
▪ Bank Reconciliation Statement	
▪ Cheque Dishonor Report	All departmental Modules, CCC
▪ Analysis on unspent amount of previous years	
▪ Various reports required for submission to Standing Committee	
▪ Liability Estimation with respect to Material Bill entry or Receipt of Material	
▪ EMD/Security/Bank Guarantee Report	
▪ Variance Report	
D] Other Requirements	
▪ Creating account no. As per National Accounts Manual which suggests a 15 digit number format and enabling migration easier whenever required.	
▪ Demand details for various departments and approved values in budget for different departments should be viewed by account official.	
▪ Integration of Account department with various public/private banks.	
▪ Bank guarantee register	

3.9. Audit Module

Functionality	Integration required with
A] Departmental Process	
▪ Pre-Audit of Tenders, Estimates	Accounts
▪ Audit Para Entry	Accounts
▪ Post Audit of the Departments	
▪ Inspection of Contractor & Supplier Bills	Accounts
▪ Inspection of Other Bills like Telephone Bills	
▪ Inspection of Advance Adjustment proposals	
B] Reports	
▪ Department-wise Budget Provision v/s Expenditure Report	
▪ Status report on Audit Para	
▪ Various statutory reports to be submitted to Standing Committee	Accounts
▪ Exception Reports (w.r.t. deletion of records, adjustment entries, etc.)s	Accounts, Other Modules

3.10. Solid Waste Management Department

Functionality	Integration required with
A] Area details	
▪ Area information (Zone / Ward / Colony / Society) ▪ Population details ▪ Volume of the Solid waste (Recycled & Non Recycled) ▪ Resources required (Manpower, Vehicle, Equipment) ▪ Collection procedure (i.e. Primary : Residential & Commercial collection, Gate to Dump / Transfer Station; Secondary : Community Bin to dump site / transfer station)	GIS, Property Tax Module, Fleet Management, GPS Software Solution
B] Garbage Collection Scheduling	
▪ Assign SWM Vehicles to pick-up the Garbage. Route / Category wise assignment.	GIS, Fleet Management, GPS Software Solution
▪ Zone wise / Ward wise / Location-wise / Bit wise assignment of Sanitation Staff	GIS, HRMS
▪ Scheduling of garbage collection and cleaning activities with the objective of maximizing citizen friendliness on one hand and optimum use of resources on the other.	
▪ Assigning routes to SWM vehicles / Dumper placers / Compactor vehicles etc.	GIS, Central Workshop
C] Primary Garbage Collection & Disposal through weigh bridge	
▪ Record the volume of garbage collected and disposed on a daily basis. Source segregation like Quantum of waste collected with further segregation for vermiculture, Bio dispose can be kept on Monthly / Yearly basis. The same can be used for RV benefit.	Central Workshop
▪ Linkage with Garbage Bins in case of Citizen Grievance	CCRS, GPS
▪ Keeping certain Checks as per environmental regulations, like minimum frequency of lifting garbage, transportation mode, etc.	GPS Software Solution
▪ Record of garbage bin/container (Community bin) lifted as per schedule.	GPS Software Solution, GIS
▪ Record of cleaning of roads / boundaries done as per schedule	GIS
▪ Record of waste gone to process plant as per schedule	GIS, GPS Software Solution
D] Treatment of Waste & Disposal of Inert Waste at Landfill site	
▪ Reports on Input of Waste by plants, final products made by the plants	
▪ Reports on inert waste sent to the land fill site by the plants	
▪ Revenue generation to Authority from process plants (may be in the form of royalty)	GPS Software Solution
E] MIS	
▪ Monitor the deployment of pickup trucks and personnel based on the schedule originally drawn.	GIS, GPS Software Solution
▪ Generation of registers like: Contracts Register for SWM, Site Register (landfills), Contractors Register, etc.	
▪ SWM Contract Wise Status Reports, Site Wise Progress Summary, Contractor wise Performance Analysis, etc.	

Functionality	Integration required with
▪ Comparison of expenditure on SWM activities over different geographical areas, years, agencies, etc.	GIS, GPS Software Solution, Accounts
▪ Daily / Monthly reports of comparison for how much garbage has to be lifted as per target & how much garbage is actually lifted. If less lifted then reasons for the same for e.g. Breakdown / Labour problem.	GIS, GPS Software Solution
▪ Daily / Monthly status reports of waste bin process plants	
▪ MIS report for expenditure incurred on primary sweeping, door-to-door / gate-to-dump / transfer station	HRMS, Accounts
▪ MIS report for expenditure incurred on transportation	Central Workshop, Accounts
▪ MIS report for expenditure incurred on disposal	Accounts, GPS Solution Software
▪ Record of waste vehicles operating with schedule details at various regional/zonal offices & Ramp	GIS, GPS Software Solution
▪ Daily / Monthly status report of cleaning of Public urinals, toilets.	GIS, GPS Software Solution
▪ Daily / Monthly status report of action taken by Health Inspectors & Class III / IV employees assigned to each Ward offices / Zonal offices.	
▪ Mandatory reports (annual reports to GPCB, CPCB, MOEF, annual report to planning dept. of Authority)	
F] Other requirements	
▪ Capturing RFID Details of all waste collection vehicles /dumper/compactor, etc. along with details of waste collected by each of them.	GPS Software Solution, Accounts

3.11. Welfare Schemes Module

Functionality	Integration required with
Master Entry of the different Schemes - AIDS awareness - Family planning and MCH - School health program - Janani Suraksha Yojana - Jeevan Dayi Yojana - RCH programs - Self-employment slum / Non slum - Training schemes - Education - S.S.C. & H.S.C. scholarship schemes - Contributory Health schemes - ICDS immunization programs - Integrated child development project - Any other Schemes	Web Portal
Creation of Database of beneficiaries	Property Tax
Recording and accounting of the grants / funds received for implementation of various schemes	Accounts
Preparing of the budgets for the implementation of the schemes	Accounts
Allocation of work and fund required for implementation	Accounts
Recording and accounting for the expenditure incurred for the implementation of the project	Accounts
Generation of necessary reports needed to monitor the implementation of the schemes	

3.12. Human Resource Management System

Functionality	Integration required with
A] Generic Features – Mandatory requirements	
▪ System should provide for Retrospective calculations to be handled for all types of scenarios (employee joining, leaving, pay hike, promotions, etc.)	Accounts
▪ System should be able to handle all statutory regulations and maintain the details directly in the screens provided for data entry. All rules related to such acts should be preconfigured in the system.	
▪ Vendor to provide for Legal change patch to take care of any statutory changes.	
▪ System should provide the capability to upload documents of employees like certificates, transfer, promotion letters in a scanned format into the system and ability to retrieve them whenever required	Document Management System
▪ Capability to integrate with Authority web portal for employees self service	Web Portal
B] Recruitment and Manpower Planning	
▪ Facility to carry out Vertical & Horizontal recruitment	
▪ Facility to carry out recruitment for different types of employees separately viz., Officers, Special Officers, Clerks, subordinates, Sanitation Staff, etc.	Web Portal, WMS, CCC
▪ Sorting of applications received	
▪ Storage of Advertisement Published	
▪ Provision to define requirement plans (periodic) in terms of specific skills, Qualifications, experience, designation, etc.	
▪ Provision for mainstream, specialist and part time employee recruitment	WMS
▪ Provision for Dependent (legal heir) Recruitment	WMS
▪ Storing NOC from other family members	
▪ Support to analyze the cadre-wise / ward or office-wise / department – wise staff strength – sanctioned/working strength and the gap for which recruitment is required	
▪ Facility to capture the data relating to resignations / retirements / VRS / suspension / death / unfitness, etc.	
▪ Allocation of employees to various departments as mentioned in the order which they received at the time of recruitment/joining.	
C] Employee Master Data	
▪ System should be able to record and store Master Data Information for an Employee / Councilors for following areas and should be able to provide a snapshot of employee's history at any point in time on a click	
▪ Name	
▪ Address	
▪ Education Qualification	
▪ Previous Employment	
▪ Phone Numbers / Contact Information / E-Mail ID	
▪ Date of birth	
▪ Work Experience	
▪ Languages known	

Functionality	Integration required with
▪ Family Information	
▪ Employee photo, Signature, Biometrics	
▪ PAN No./ Passport / PF number/GPF No/ TAN No./ UID No. for dept.	
▪ Bank account information	
▪ Employee blood group	
▪ Property Tax No.	Property Tax Module
▪ Any other information that Authority may require should be easy to enter and report on	
▪ Employee Type– (Permanent / Temporary / contract workers / Project Based)	
▪ Employee category (SC/ST/OBC/Others)	
▪ Ex service man / Handicap / Sports man etc.	
▪ Location (HO/zone/ward/Election ward/branch)	
▪ Department	
▪ Job code/designation/ Class with scale efficiency bar	
▪ Grade/cadre (with facility for sub grouping)	
▪ Job Role (access rights to different modules will be assigned based on the roles)	
▪ Job history covering details of appointments	
▪ Departmental Inquiry details	
▪ Any other punishment details	
▪ Any awards (Puraskar) received	
▪ Details of significant work done	
▪ Health Check-up while joining the duty & as per the policy	
▪ History of election duties attended	
▪ Promotions, transfers	
▪ Trainings attended	
▪ Deputation, temporary transfers	
▪ Increments	
▪ Increment for passing of Govt. Exams.	
▪ Date of pay rate change, etc – Increment	
▪ Date of joining	
▪ Date of probation/confirmation	
▪ Date of termination/retirement/suspension(with details)	
▪ Previous employment details	
▪ Union Information (if applicable)	
▪ Compensation data including components of pay	
▪ Compensation of pay for calculation of gratuity and pension	
▪ Family photo in case of pension, nominee photograph.	
▪ Capture Biometric Details of employee. (Fingerprints of each finger, retina scan, etc.)	

Functionality	Integration required with
▪ Provision to define Roles and Designations as per Authority requirements and assigning employee to the same.	
▪ Uniform, Equipment given (period-wise & quantity-wise)	
▪ Quarter allotted (if any)	Asset Management
▪ Roster functionality for recruitment and promotion applications.	
▪ Capturing physical disability of the person (if any) at the time of recruitment along with the type and percentage of disability.	
D] Payroll Management	
▪ Ability to define flexible periods such as day, week, month for pay calculation	Accounts
▪ Ability to enable multiple payrolls that are generated based on employee's assignment	
▪ Ability to define payroll for pensioners	
▪ Ability to define the employee bank to credit the salary	
▪ Facility for Electronic Clearing system (ECS)	
▪ Bank-wise / Bank branch wise summary statement	
▪ Ability to provide automatic calculation of deductions / earnings based on leave, bonus declaration, GPF Loan, Home Loan, Computer loan , tax deductions, Quarter Rent - HRR (person won't be eligible for HRA), etc.	
▪ TA / DA submissions	
▪ Medical reimbursements	
▪ Confirmation of any employee loan (EMI start date & last date)	Accounts
▪ Ability for rule based pay calculation in case of pay hikes / Pay Commission with retrospective effect	Accounts
▪ Ability to define unlimited pay elements/types. These pay elements should be classified as Earnings, Reimbursements, deductions, tax deductions, PF, etc. Pay elements should be also classified as Recurring & non-recurring	
▪ Ability to apply the payment rules at personal / department / designation / organization level	
▪ Ability to allow exception definitions at employee / designation / department level	
▪ Ability to define all India specific taxation rules.	
▪ Ability to automate increments (based on pre-defined rules – employee / designation / department / organization specific)	Accounts
▪ Facility to run payroll processing any number of times before authorization to ensure accurate pay calculation	Accounts
▪ Provision to allow deductions for specific purposes (like earthquake relief fund, CM relief fund, etc.)	
▪ Ability to share information with Accounting module of the current e-Governance solution with respect to payment or receipt related transactions	
▪ Ability to share information with the Accounting module of the current e-Governance solution for all necessary Double Entry Accounting related information (salary payable at the end of financial years, etc.)	
E] General Provident Fund Management	

Functionality	Integration required with
▪ Issuing GPF no. to employees	Accounts
▪ Application acceptance for advances / Loan against GPF	
▪ Scrutiny of the applications	
▪ Payment of Advance / Loan to Employees	
▪ Interest Rate for GPF calculation	
▪ Repayment Installment adjustment against salary	
▪ Generation of various MIS (Monthly / Yearly)	
F] Employee Promotions / Transfers and Development	
▪ Transfers	
▪ Time bound Promotions	Recruitment
▪ Grade and Pay changes	Payroll, Accounts
▪ Ability to create standard career paths in the Corporation in terms of various possible moves from the current level / grade in the Corporation	
▪ Ability to define grade advancements within a level on the basis of time based as well as merit based criteria	
▪ Ability to define the rules for promotion eligibility in terms of tenure, consistent achievement of high performance grades, etc.	Recruitment, Manpower Planning
▪ Ability to define additional rules specific to service in terms of suspensions, disciplinary actions	Departmental Inquiry
▪ Facility to intimate employees of promotion / rejection through mail / workflow / letters	SMS Gateway
▪ Facility to create offer letter on promotion	
▪ Ability to define short / long term goals for employees and provide a framework to assess and update completion of the same	
▪ Ability to identify key positions for the purpose of succession planning	
▪ Ability to plan for vacancy of the key position in advance	
▪ Identify the gaps / developmental areas between the slated employees and requirements of the key position	
▪ Maintenance of complete history of employee transfers since his recruitment	Recruitment, Manpower Planning
▪ Transfer/redeployment of officers based on requirement/sanction strength of different regions/zones	
▪ Generation of seniority list	
▪ Posting / transfer of officers upon their promotions	
▪ Maintenance of records for officers transferred out of parent state and also officers to be transferred back to home state on completion of required tenure	
▪ Maintenance of transfer records of specialist transfer, identification of vacancies and issue of transfer orders based on the recommendations received from the respective specialist departments	
▪ Provision to maintain lateral transfer details and transfers on promotion	

Functionality	Integration required with
▪ Generation of list of eligible staff members for transfer based on the user defined criteria (like those who in 3 years' service at one place, those who working more than 10 years in one region, those who have not worked outside the state in a particular scale or overall position	
▪ Maintenance of exemptions given in transfers with a facility to record the reasons for the same	
▪ Provision to record the transfer orders cancelled/deferred/modified and follow up with the respective regional/zonal offices for implementation	
▪ Capture of details of officers on deputation to outside agencies, etc.	
▪ Without transfer allotment (salary at original dept.)	
▪ Mass allotment for programmes like elections, pulse polio etc.	
G] Time Management and Leave Management	
▪ Support attendance entry from various sources such as direct entry, rule-based and automatic (through biometric device / swipe card / smart card)	Accounts
▪ Definition and maintenance of leave calendars for different types of leave depending upon the scales of the employee	
▪ Provision to maintain all types of leave like CL, PL, ML SL extra-ordinary leave, special leave etc	
▪ Ability to maintain leave eligibilities for each type of leave depending on the rules specified by Authority	
▪ Facility to identify Collisions when Employee goes for Leave and take appropriate action	Accounts
▪ Ability to maintain rules for leave taken in terms of rules for availing leave, encasing leave, accrual of leaves, lapsing of leaves, ceilings for accumulation of leaves, rules for combination of leave types, etc.	Accounts
▪ Ability to record actual leaves taken	
▪ Ability to calculate actual leave balance at any point of time	
▪ Link Leave management to payroll and employee history	
▪ Provision to accounting of leave including automatic credit of leave and also provision with manual credit / debit / modification / cancellation etc.	Accounts
▪ Leave cancellation and leave extension / amendments advancement, postponement of leave	Accounts, WMS
▪ Supports extra-ordinary leave on loss of pay	Accounts
▪ Avail Leave / carry-over processes administration as per the statutes laid down by the government / Authority	
▪ Incorporating second level authentication mechanism such as fingerprint scanning / retina scan for applications such as attendance, approval of various files, etc. for all the departments.	WMS
H] Performance Appraisal	
▪ Capability to create Performance documents for employees depending on the cadre / grade in the organization	
▪ Ability to define competency wise / parameter wise desired levels of performance for each cadre / grade in the organization	

Functionality	Integration required with
▪ Ability to define proficiency descriptions for each parameter for each cadre / grade so as to ensure that the same measures of performance are communicated to the appraiser as well as the appraisee	
▪ Facility to attach different rating model (5 point scale, 7 point scale) depending upon the cadre / grade in the organization	
▪ Ability to define the period for which appraisal is being carried out	
▪ Capture appraisal details as given by the appraising authority, reviewing authority	
▪ Support parameter wise ratings, final ratings, strengths / weakness and suggestions / recommendations for improvements by the appraising/reviewing authority	
▪ Facility to give weightage to each parameter and points against each rating attained along with remarks for the same	
▪ Facility to consolidate the overall points and calculate an overall grade for the appraisee	Accounts
▪ Facility to import Short / Long term goals (particularly at officer level and above) in the Performance appraisal document	
▪ Support maintenance of history of performance appraisals and promotions	
▪ Support maintenance of automatic release of time based increments	
▪ Release of increments for qualifications acquired	
▪ Increments released should automatically be integrated with the payroll module and other relevant modules	
▪ Support generation of increments due for each month or for user defined period for employees – cadre wise/scale wise/other user defined combination	
▪ Support to generate reminder letters / mails / workflows to the employees / appraising authorities in case of non-submission of self-appraisals, etc.	SMS Gateway
▪ Support memo letters / mails / workflows to be issued to the employee in case of unsatisfactory performance	WMS
I] Departmental Enquiry	
▪ Ability of software to record the details of sanction given by Commissioner or Additional Commissioner for departmental enquiry.	
▪ Ability of software to note charges against the employees	
▪ Ability of software to record the clarification given by the employee under charge	
▪ Ability of software to record the appointment of Enquiry Officer & Presentation Officer	
▪ Ability of software to record the enquiry scrutiny details like history, evidence, papers submitted, relevant documents , photographs etc.	
▪ Ability of software to check if there is any corruption/police case being registered against the employee.	
▪ Ability of software to record the 'Finding Report' of Enquiry Officer & Presentation Officer	
▪ Ability of software to record the 'Explanation details' given by the employee	
▪ Ability of software to record the details of ' Proposal for action' submitted to commissioner	

Functionality	Integration required with
▪ Ability of software to record the order given by the commissioner	
▪ Ability of software to generate the 'Show Cause Notice/Enquiry Notice'	
▪ Ability of software to record the clarification given by the employee under charge sheet	
▪ Ability of software to record the punishment order or penalty	
▪ Ability of software to record details of suspension & suspension order.	Accounts
▪ Ability to incorporate mercy plea details (if any) issued from the standing committee.	
▪ Ability of software to capture details of resetting of service	
▪ Ability of software to record the 'enquiry start date' & 'enquiry finish date'	
▪ Ability of software to record the inward/outward details like inward/outward number & date	
J] Reporting	
▪ Reporting capabilities for AdHoc Reporting	
▪ Reports on Demographic	
▪ Reports on Vacancies	
▪ Report on Employees Salary Details	
▪ Report on Leave Availed	
▪ Report on Leave Entitlements	
▪ Employee Attendance List for a Business Event	
▪ List of the Departmental Enquiries being conducted at a point of time or for a specific time with drill down option to get further details on the enquiries	
▪ Headcount Report	
▪ Report on time spent in a grade / employee tenure	
▪ Transfer List	
▪ Roster report for recruitment and promotion application.	
▪ Form 16 with Form 12 BA	Payroll, Accounts
▪ Report for 'E' forms	Payroll, Accounts
▪ Income Tax related reports	Payroll, Accounts
▪ Summarized Pay Register	Payroll, Accounts
▪ Form 24	Payroll, Accounts
▪ Provident Fund Returns: Monthly returns to the Regional Provident Fund Commissioner for joining (Form 5) or leaving employees (Form 10) and the contributions paid (Form 12A) as well as monthly returns for Pension contributions for exempted trusts for joining (Form 4) or leaving employees (Form 5) and the contributions paid (Form 6)	Payroll, Accounts
▪ Professional Tax returns	Payroll, Accounts
▪ Form 6 and Form 7, the Quarterly / half yearly returns to be generated by the payroll for the eligible employees with the relevant annexure listing the employees and the amounts earned and deducted	Payroll, Accounts
▪ Facility to configure and use the system to develop additional reports on a need basis with tools like Crystal Reports	
K] Additional Features	

Functionality	Integration required with
▪ Ability to define organizational events like training, Training records. Record of Examinations, Certificates after passing exams, seminars, workshops and capture the attendance for the same	
▪ Maintain comprehensive record of employee grievance	CCRS
▪ Track disciplinary action taken against employees, capturing the costs incurred along with the activities undertaken as part of the disciplinary action. Automate salary deductions, if proposed.	Departmental Inquiry, Accounts
▪ Recovery from employees along with reasons & facility to divide it in installments.	
▪ Reports on trainings / workshops / seminars attended by employee.	
▪ Welfare process for class IV employees.	
▪ Jobs on compassionate grounds for Manhole workers and non-permanent class – IV staff.	
▪ Fixed amount to be given to the class – III and class –IV workers in case of accidental death on job.	HRMS, Accounts
▪ Termination Details of each employee to be incorporated. (Suspension, Normal Retirement, Compulsory Retirement, Voluntary Retirement, etc.)	HRMS, Accounts
▪ Fire & Emergency Services.	All Departmental Modules
F] Other Requirements	
▪ Data Porting / Data Entry Suite	
▪ E-Mail / SMS to be sent to all / selected categories / Selected employees ▪ Pay-Slips / Regular Communications ▪ Urgent Communications ▪ Notices	SMS Gateway / Web Server

Note: HRMS Module should include details of all the employees affiliated/working under the head of Authority.

3.13. Employee Self Service Module

Functionality	Integration required with
A] Employee Self Service	
▪ Ability to allow employee request to modify personal, skill, family details	HRMS, Workflow Management System, SMS Gateway, Hospital Management System, Accounts
▪ Employee should be able to make leave requests	
▪ Supervisory officer should be able to get an alert when any Self Service Request of sub-ordinate staff is received by him	
▪ Supervisor authorization of modification of the employee requests or leave application	
▪ Employees should be able to view the status of their requests	
▪ Ability to facilitate self-appraisal by employees	
▪ Ability to undertake online appraisal of the sub-ordinates (CRs)	
▪ Ability to define customized NOC requests (like NOC for Passport application, NOC for foreign travel, retirement benefits, etc.)	
▪ Various health benefits available to employee	
▪ Register Employee Complaints	Grievance Redressal
▪ Allow employees to request any other information from any other department	
▪ Online submission of annual property statement (Asset Declaration)	Accounts
B] Reports	
▪ Salary Details	HRMS, Payroll/accounts
▪ Leave Availed	Leave Management
▪ Income Tax related reports	HRMS, Accounts, Payroll

3.14. Legal Module

Functionality	Integration required with
A] Masters	
▪ Advocates, their fees	Accounts
▪ Court Master	
B] Case Management	
▪ Registration of new cases, allocate advocate, allocate Authority officer	HRMS
▪ Facility to attach various documents related to the case	
▪ Entry of Date of Hearing	
▪ Capture Court Interim order details received from court	
▪ Check for court commission order issued from court	
▪ Alerts to officers w.r.t. hearing date (Legal/any other affiliated dept.)	HRMS, SMS Gateway, WMS, All Departments
▪ Entry of hearing details	
▪ Reply/Affidavit filed at court (by the department)	Document Management System
▪ Interim Order Details	Document Management System
▪ Capture of judgment	
▪ Details of payments to the advocates	Accounts
▪ Linkage to the departmental data	Departmental Modules
▪ Linkage to GIS to capture location reference for cases	GIS
C] Legal Opinion on various departmental queries, agreement formats	Document Management Module
D] MIS	
▪ Case Pendency reports (Department-wise / advocate-wise / Officer-wise)	HRMS, WMS
▪ Reports w.r.t. Cases won / Lost / Appeals made	
▪ Payments to the Legal Advisors	Accounts
▪ Repository for various act and provision with search option	
▪ Integration / Link to Andhra Pradesh government site for GR references.	
▪ Repository of all the cases since 1950 by High court and Supreme Court with search feature.	
▪ Generate court interim order reports along with status of all registered cases.	
E] Other Requirements	
▪ Data Porting / Data Entry Suite	

3.15. Project Systems (Engineering) Module

Functionality	Integration required with
A] Project Initiation	
▪ Defining New Project	
▪ Selection of Department, Officers for scrutiny	HRMS
▪ Selection of Budget Code	Accounts
B] Project Estimation	
▪ Identification of different items, defining units	
▪ Selection of SOR / Market Rates / DSR /ESR / WSR Rates	Document Management System
▪ Preparation of Measurement Sheet	Accounts
▪ Addition of specifications not included in Standard DSR (for special items)	
▪ Preparation of Abstract sheet	
▪ Preparation of Rate Analysis Sheet	
▪ Preparation of Recapitulation Sheet	
▪ Defining various Milestones / Time limit	
C] Technical Sanction	
▪ Workflow for Technical sanction as per chart of competent authorities	Workflow System
▪ Workflow system to support To & Fro movement of proposal/file	
D] Administrative Sanction	
▪ Workflow for Administrative sanction as per Delegation of Powers(DEP)	Workflow System
▪ Workflow system to support To & Fro movement of proposal	
▪ Negotiation	Access rights to be given as per DEP
E] Tendering	
▪ Generation of information for press Advertisements	
▪ Check-list for Tender Notice	
▪ Special conditions for contract if any	
▪ Publish Tender Notice on Web Portal	Web Portal
▪ Publish Tender Document on Web Portal	
▪ Reports to assist Tender Document preparation	
▪ Check-list for Tender Terms & Conditions	
▪ Purchase of Tender Documents	Accounts, Web Portal, CCC
▪ Submission of bids	Manual
▪ Technical bid evaluation	
▪ Cross-check of vendors with the approved Vendor list of Authority and their previous records	
▪ Commercial bid evaluation	
▪ Cross-check of rates with similar projects in past	

Functionality	Integration required with
▪ Award of contract	
▪ Milestone entry	
F] Project Execution	
▪ Project Scheduling	
▪ Measurement Book Entry and it's movement diary	Accounts
▪ Monitoring of progress	
▪ Quality Control (PMC / TPIA report)	
▪ Notices to agencies / vendors (for delay, for poor quality, any other reason)	
▪ Levy of Penalty	Accounts
▪ Agencies Black-listed / restricted for certain period	
G] Billing & Completion Certificate	
▪ Running Account Bills	Account
▪ Billing for Extra / Excess items	
▪ Completion / utilization certificate	
H] MIS Reports	
▪ Project wise comparison of Budgeted Expenditure Vs. Actual Expenditure	Accounts
▪ Milestone Monitoring Report	GIS
▪ Measurement Sheet / Abstract Sheet / Rate Analysis Sheet / Recapitulation Sheet	
▪ Technical Bid Comparison	
▪ Financial Bid Comparison	
▪ Billing Information	Accounts
▪ Project Summary Sheet	
▪ Reasons for delay in achieving milestones. The responsible parties to be identified like any Authority Department or Contractor.	
▪ Reports / Alerts through other systems for New Projects o Building Permission Module o Grievance Redressal Module o Alerts for Road Re-surfacing / Repairing	GIS
▪ Cross-departmental information as alerts while defining new projects o E.g. : Water Department should get alerts for Pipeline laying, if the Road (location, measurement) is being prepared / re-surfaced / Grouting / Paving	GIS, Integration of all modules with this.
I] Other Requirement	
▪ Registration of contractors/Suppliers	
▪ Up-gradation of contractors data / Blacklisting of contractors	
▪ Contractors Register	
▪ Confidential Register of Contractors/Suppliers	
▪ Road register (Traffic (PCU) / Road history / Defect liability)	
▪ PWD Register (Works Manual / Account Manual)	

Functionality	Integration required with
▪ Manual followed by dept. for implementation of projects (IRC / CPHEO / WHO / ISO / etc.)	
▪ Bridges register (history / annual maintenance / Continuous monitoring / details of PCU)	
▪ Monitoring of Sewerage treatment plants. History & all the relevant data (Monthly report of influent & effluent characteristics of sewage, electricity consumption, BOD, COD, GPCB reports, Third Party Reports, etc)	SWM
▪ Revenue generation from STP	
▪ Expense for O&M of Sewerage System o Collection Cost o Sewage Treatment cost o O&M of Pumping Station	
▪ Monitoring of Drainage Pumping Stations. History & all the relevant data (Monthly report of functioning, electricity consumption, etc)	
▪ Monitoring of Water treatment plants. History & all the relevant data (Monthly report of raw & treated characteristics of water, electricity consumption, Central Laboratory / Health Dept., Third Party Reports, etc)	
▪ Monitoring of Water Pumping Stations. History & all the relevant data (Monthly report of functioning, electricity consumption, etc)	
▪ Expense for O&M of Water Distribution System o Raw water cost o Production cost o Distribution Cost	
▪ Monitoring of Hot mix plant (material stock, consumption, TPIA reports, etc)	

3.16. Hospital Management System

Functionality	Integration required with
A] Registration of Patients & Inquiry	
▪ Preparation of Case Papers	
▪ Classification of Case (Emergency, Normal, etc.)	
▪ Capture photo of Patient along with case papers.	
▪ Capture Type of Patient, National Programs and the schemes with which the patient is associated for pursuing treatment.	
▪ Payment of Registration Fees	Accounts
▪ Patient Inquiry	
▪ Date for next visit should be automatically generated. Facility for manual setting of date if patient does not turn up.	
▪ Facility to edit patient information to be provided to authorized doctors	
▪ Templates for different departments (e.g. Lab Management, Radiology, OT, etc.) to be prepared as required by the departmental authority.	
B] OPD / IPD Management	
▪ Doctor Managing the OPD / IPD	HRMS
▪ Consultation / Investigation Detail	
▪ Medicine Proposed	
▪ Follow up of OPD	
▪ Billing	Accounts
▪ Facility to request for Extra Bed	
▪ Provisional diagnostic details	
▪ Final diagnostic details after proper consultation and investigation (lab reports, other reports, etc.) of the patient, to be inserted at the time of discharging patient.	
▪ Consent Form	
▪ CSSD Checklist to be filled on mandatory basis	
C] Ward Management	
▪ General / special / ICU / NICU	Accounts, Departmental Modules
▪ Consent Form	
▪ Patient Allocation to various Beds	
▪ Daily visit report	
▪ Outcome & Discharge Summary	
▪ Prescribing Diet and Nutritional Details to patient ward wise.	
▪ Tender Document Fees	
▪ Billing at the time of Discharge	
▪ CSSD Checklist to be filled on mandatory basis	
D] OT Management	
▪ OT Scheduling	
▪ Capture timings for OT	
▪ Prepare OT list as per the timings defined for OT.	
▪ Surgery Details	

Functionality	Integration required with
▪ Dialysis	
▪ Doctor Details	HRMS
▪ Output Details	
▪ Drugs/Disposables consumption	Material Management
▪ Provisional Bill Generation	
▪ Billing	Accounts
▪ Prepare Special Consent draft as specified by authorized officials.	
▪ Preparing Surgery Consent draft as required.	
▪ Capture anesthesia and other miscellaneous details related to the same	
▪ Patient Safety	
▪ CSSD Checklist to be filled on mandatory basis	
▪ Non-surgical procedures (angioplasty, etc.)	
E] X-Ray & ECG / Radiology & Imaging Management	
▪ Case details	
▪ Records & Data management (CT scan, MRI, Ultrasound, etc.)	
▪ Generation of reports for PNDT & ANC	
F] Special Disease National Programs (ARV / TB / AIDS)	
▪ Case details	
▪ Location	GIS
▪ Forms	
▪ Auto Reports generation based on predefined time schedule	
G] Lab Management	
▪ Lab Scheduling ▪ Sample Collection details ▪ Inward details/history ▪ Technician details ▪ Report preparation ▪ Record management ▪ Pathology reports ▪ Reports on various types of test conducted ▪ Provisional Bill Generation ▪ CSSD Checklist to be filled on mandatory basis	SMS Gateway for Pathology Report
H] Medical Board / Medical Fitness	
▪ Employee details	HRMS
▪ Inward, Case preparation	
▪ Test reports	HRMS
▪ Issuance of certificates (Templates to be prepared for issuing fitness/unfit certificate)	HRMS
I] Student Management	
▪ Attendance	HRMS
▪ Shifts	
▪ Posting of students	
▪ Training Certificate	

Functionality	Integration required with
▪ Apprentice/Training	
J] Other Details	
▪ Casualty Case Details	
▪ Utilization Reports for Nurses / Doctors	HRMS
▪ Capture of Patient Feedback	
▪ Medical Audit	
K] Knowledge Centre	
▪ Patient Information on Web-site	Web Portal
▪ Area wise list of Multi Special Hospitals with contact numbers	Web Portal
▪ Area wise list of Specialist Doctors with their addresses and contact nos. of their Clinics.	Web Portal
▪ Area wise list of Ambulance services & Numbers	Web Portal
▪ Area wise list of Crematoriums	Web Portal
▪ Health Bulletin	Web Portal
L] Pharmacy Management	
▪ Medicine Inward / Outward	
▪ Stock Management	Materials Management Module
▪ Acceptance of Payments	Accounts
M] Epidemic Control	
▪ Water Sampling	
▪ Reporting of cases by surveillance centers UHCs, Hospitals, Path labs	
▪ Daily Compilation and alerts	
▪ Weekly and monthly reporting	
▪ Monitoring of new diseases like Swine Flu, etc.	
▪ Details of Patients visiting Central Control Unit with details of age, sex, ailment details, medication given, etc.	
N] Medical Record Room (access to be given to RMO only)	
▪ Patient Records	
▪ Lab Records	
▪ Imaging Records	
▪ Medico-legal case details	
▪ Issuance of certificates (Templates to be prepared for issuing fitness/unfit certificate)	
O] MIS	
▪ Patient Analysis	
▪ Casualty Case Details	
▪ Occupancy reports	
▪ Patient Feedback Analysis	
▪ Generation of Daily/Monthly/Quarterly reports	

Functionality	Integration required with
▪ Generation of reports required for Governmental bodies for AIDS control society (GSACS), Vaccination, TB, ARV, PNDT, ANC care, various diseases, Birth & Death statistical reports.	
▪ Generation of monthly expenditure for procurement 'Tasalmat' reports	Accounts
▪ Code Numbering for hospitals for easy collection of reports	
▪ Provision for cumulative reporting for each hospital	
▪ Stock report for each vaccine	Material Mgmt.
▪ Daily shift register of doctors hospital wise	HRMS
▪ Daily / monthly report of operations hospital wise	
▪ Treatment details with disease, medicine given in OPD	
▪ Daily cash collection report at each OPD	Accounts
▪ Customized statistical reports of daily patient visits at each OPD	
▪ Statistical comparison report PNDT figures of Vizag city with International / National Cities	
▪ Analysis of the cases on the basis like Dog bite, Malaria, Waterborne, air borne, communicable disease, etc.	
▪ Reports to indicate possible breeding spots, based on the cases from particular geographic area / demarcation of area.	GIS
▪ Epidemic diseases report	
▪ Cost & Expense report	Accounts
▪ Case history to be generated for each patient which can be printed and can be saved as PDF/DOC document.	
▪ Generating different cases report on the basis of their classification	
▪ Generate template for preparing various reports.	
P] Contract Management	
▪ Vendor Details	
▪ Equipment Details (fire safety, medical equipments, etc.)	
▪ Annual Maintenance Contract Details	
▪ Maintenance Scheduling for all Biomedical Equipments	
▪ Log Sheet	
▪ Stock Management (Spares / Consumables)	
▪ Operation Theatre Maintenance	

Note:

- The Bidder has to integrate the proposed application software solution with PACS system or DICOM supported medical equipments.
- PACS and DICOM supported system would be provided by Authority during the tenure of the project.

3.17. Municipal Secretary Module

Functionality	Integration required with
A] Executive Wing Database	
▪ Database of members of various committee, corporators, mayors etc	Web
B] Agenda Preparation	
▪ Preparation of Agenda by Department & submission to Municipal Secretary Dept.	Projects
▪ Submission of proposals from various Counselors	
▪ Selection of Type of Meeting (General Body / Standing Committee / Special committee / Tree Authority committee / Name committee / Ward Committee / special committee's like Women & Child welfare committee, Law committee & City improvement committee/Emergency)	SMS Gateway
▪ Selection of different Agenda received for a meeting	
▪ Schedule of meetings of various committees	
▪ Generation of Agenda Copy	
▪ Issue of Agenda to Members & Administration after approval.	Work-flow
▪ Issuance of letters received from the office bearers to various departments.	WMS
C] Minutes of Meeting	
▪ Capture of Proceedings	
▪ Capture of Attendance of the members	
▪ Printing of Minutes after approval	Work-flow
D] Resolution Preparation	
▪ Preparation of Resolution and/or Circulars	WMS, Web Portal
▪ Distribution of Resolution	Document Management System
▪ Publishing of resolutions on Web Portal	Web Portal
E] MIS	
▪ List of issues discussed department-wise & committee wise in a specific time period	
▪ Attendance Details	HRMS
▪ Resolution/Circular Details	
▪ Data required for the preparation of annual report (Total number of resolutions passed, meetings held etc)	

3.18. Asset Management

Functionality	Integration required with
A] Classification of Assets	
▪ Immovable Assets o Land o Building o Roads, Footpaths o Bridges, Culverts, Flyovers, Subways & causeways o Drains including underground drains o Water Works Distribution o Public Lighting System o Lakes and Ponds o Capital Work-in Progress	GIS, Project Systems
▪ Movable Assets o Plant and Machinery – including machinery of Water Works & Drainage, Road dept. machinery o Vehicles o Furniture & Fixtures o Office Equipments o Other Equipments o Live Stock	Central Workshop System
▪ Investments	Accounts
▪ Capture Various details for the Assets o Ownership o Cost Details (construction / Purchase / Transfer) o Depreciation Principles o Other details to arrive at Current Value	Accounts
▪ Preparation of Opening Balance for Asset Valuation	Accounts
B] Asset Transactions	
▪ Purchase of New Assets	Municipal Secretary, Projects, Accounts, WMS
▪ Acquisition of Land	
▪ Asset Sale	
▪ Investment on Assets (like construction of new floors, road re-surfacing, etc.)	
▪ Insurance Details	
▪ Insurance Claim Related Information capture	Accounts
C] MIS	
▪ Asset Register	GIS
▪ Revenue Report	Accounts
▪ Outstanding Register	GIS, Accounts
▪ Search facility for various information (like search for name of road)	GIS
D] Other Requirements	
▪ Data Porting / Data Entry Suite	Accounts

3.19. Land & Estate Management

Functionality	Integration required with
A] Land Management	
▪ Proposal for Land Acquisition	GIS
▪ Scrutiny of Land Details	WMS, Municipal Secretary Module(committee approval)
▪ Valuation of Land	Accounts, Property Tax
▪ TDR Process & Possession of Land	
▪ Transfer of Details to Concerned Department (Bhavan for Construction, Other department for Information)	Legal, Project Systems
B] Estate Management	
▪ Creation of Record in the Estate Register ○ Hand-over from other agencies ○ Hand-over by Builders ○ Construction by Projects Dept.	Project Systems, Building Permission Module
▪ Issuance of Municipal Property on rent / lease	Accounts, Property, GIS
▪ Generation of Bills	
▪ Acceptance of Payment	
▪ Renewal of Rent / Lease agreement	Legal, GIS
▪ Allotment of House to the employee	HRMS
▪ Maintenance of Property on Contract	GIS
▪ Maintenance Inspection report	GIS
C] MIS	
▪ Authority Land Register	GIS
▪ Land Acquisition related reports	GIS
▪ Revenue Reports for Estate on Rent / Lease	GIS, Accounts
▪ Outstanding Register for Estate on Rent / Lease	GIS, Accounts
▪ Top Defaulters List	
D] Other Requirements	
▪ Data Porting / Data Entry Suite	Accounts

3.20. Materials Management

Functionality	Integration required with
A] Masters	
▪ Categorization of Stores o Central Stores o Central Medical Store (CMSO) ➢ Hospital Stores ➢ Biomedical Engineering Store ➢ General Stores (issuing stationery and non-medical materials) ➢ Electrical Stores ➢ Civil Stores o Street Light Department Stores o Water Supply & Drainage Dept. o Roads & Building Dept. o Central Workshop Stores Dept. o Dead stock Register (for movable assets)	Accounts
▪ Defining Various Items under each category	
▪ Approved Vendor List of Authority along with their details	Accounts
▪ Price-list for the Rate Contract Items	
B] Rate Contracting or Individual Orders	
▪ Tendering	Accounts
▪ Sanction from Standing Committee	Municipal Secretary
▪ Proposal submission for Individual Orders	Workflow Management System
▪ Purchase Orders	
C] Indent Processing	
▪ Facility to each department to indent material	Accounts
▪ Issue of Material by Stores Staff	
▪ Order to vendor by Stores Dept./ staff	Accounts
▪ Material receipt forecast	
▪ Reminder to vendor in case of delay in delivery	SMS Gateway
▪ Receipt of Material, Stock Updation, Capture of Sr. No., Batch No.	
▪ Capture of Date of Manufacture & Validity Date for Food / Medical Items	
▪ Maintenance of Reorder level i.e. procurement after reaching reorder level.	Accounts
▪ Payment to Vendor	Accounts
D] Disposal of Dead Stock	
▪ Department-wise submission of details	
▪ Tendering by Stores Dept.	Portal, Accounts
▪ Disposal of Dead Stock	Accounts
E] MIS	
▪ List of Vendor-wise / Material-wise orders	
▪ Material-wise, Department-wise consumption report	

Functionality	Integration required with
▪ Disposal of Dead Stock	Accounts
▪ Status report to department w.r.t. their order	
▪ Comparison of price bids with history prices	Accounts, Central Stores
▪ Alerts if the Batch Nos. or Sr. No. is not in order	
▪ ABC Analysis, EOQ analysis, Min order, Max. order etc	
▪ Work Completion Report	
▪ Work Comparison Report	
▪ Demand & Issuance Comparative Report	
F] Other Requirements	
▪ Data Porting / Data Entry Suite	
▪ Login to suppliers to update their status	
▪ Estimation copy to be incorporated in Budget estimation.	
▪ Stock details of materials at all departments to be shown while issuing new stock for all the materials from Central Stores.	
▪ Demand Details to be created online by all departments, in case the material isn't available tender to be generated by that particular department.	WMS, Procurement Module
▪ Release vendor's EMD	WMS
▪ Intimate vendor about receipt of materials at central stores	SMS Gateway

3.21. Central Workshop Module

Functionality	Integration required with
A] Vehicle Scheduling & Fuel Management	
▪ Vehicle Scheduling	Asset Module
▪ Assigning Driver	HRMS
▪ Re-filling of Fuel	
B] Vehicle Tracking	
▪ Identification of Vehicles for Tracking	Asset Management System
▪ Online Tracking of Vehicles (Start-time, speed indicator, idle time, end time)	GIS, GPS
▪ Linking of SWM vehicles with Container Sites / Bins, Dumping Ground / Transfer Stations / Processing Plants / Land-fill sites	GIS, GPS
C] Vehicle Maintenance	
▪ Entry of the reason for repair	Asset Module
▪ Approval from the authority	Document Management System, Accounts
▪ Vehicle Issuance details	
▪ Receipt of Vehicle, entry of repair work details	
▪ Purchase of New Items (like Tyres, Battery, etc.)	Asset, Accounts
▪ Insurance Cross-check & RTO Validation	
D] MIS	
▪ Department-wise / officer wise Vehicle Inventory	Asset Management System
▪ Fuel consumption report for various vehicles	GIS, GPS
▪ Route Tracking for SWM Vehicles, cess pull tankers, water tankers, fogging machines, jetting machines, super suckers etc.	GIS, GPS
▪ Analysis of Time spent by SWM vehicles while idling	
▪ Average Fuel expenditure for various vehicles (based on the mileage & traveled distance)	
▪ No. of trips made to the Dumping Ground	
▪ System Alerts o If the petrol expense claimed by the driver is more than system calculated o If No. of trips made to the Dumping ground are less than proposed o If any particular Dust Bin was not covered	
E] Other Requirements	
▪ Data Porting / Data Entry Suite	

3.22. Web Portal

Functionality	Integration required with
A] Home Page	
▪ Message from Mayor, Commissioner	
▪ Vision, Mission, Objectives	
▪ Link to various sub-sections o City Information o Online Services o About Authority o Projects o Citizen Grievances o RTI	
B] City Information	
▪ History of Vizag	
▪ Tourist Locations	
▪ City Map with citizen related GIS information	GIS
C] About Authority	
▪ Administrative Information	
▪ Information on Elected Representatives, Various Committees	
D] RTI ▪ Names of PIO. ▪ Departments/Wards: Intro, Objectives, responsibilities, powers & duties of officers, employees with gross salary, activities, time limit, directory with telephone no. ▪ Committee: Members, purpose, type, freq. of meeting, docs available for public. ▪ Projects/ Activities: Budget head, work activities, allocated amount, current statistics. ▪ Details of concessions, subsidies given, computerization done in various depts. ▪ Integration required for updation of data for RTI with projects, accounts, HRMS, Fleet, material, asset. ▪ Scope as per RTI Act 2005 sec. 4(1).	Projects, Accounts, HRMS, Material Mgmt., Fleet Mgmt., Hospital Mgmt., Asset Mgmt.
▪ Opinion Poll	
▪ Photo Gallery	
▪ Tenders	Accounts, Projects
▪ FAQ's	
▪ Emergency Information	
▪ Employee Login using LDAP	HRMS, Associated Department
▪ Feedback	HRMS
▪ Contact Us	
E] Online Services	

Functionality	Integration required with

▪ Application acceptance for various services / certificates
  o Birth / Death Certificates
  o Duplicate Bills
  o Building Permission related services
  o Water Connection
  o No Dues Certificates
▪ Vendor Registration
	Accounts, Corresponding Module, CCRS

▪ Downloading of Forms	

▪ Online Tendering
  o Sale of Tender Forms
  o Acceptance of Tenders	

▪ Complaints
  o Acceptance
  o Status Tracking	

▪ Status on Applications / Complaints	
▪ Payment Details, Bill Details	
▪ Online Payments	
▪ Self-Assessment of Property Tax	Property Tax Module

3.23. Procurement Module

Functionality	Integration required with
A] E-Tendering Web-Site Functionality	
▪ Firms should be able to register with various essential data	Web Portal, Payment Gateway
▪ FAQs for all tender related queries	
▪ Registered firms should be able to view various published tenders and essential information in user friendly manner	
▪ Secure Login authentication	
▪ Auto-generation of various communications to the registered bidders (SMS / E-Mails)	
▪ Creation of discussion forum	
B] Tendering Functionality	
▪ Raise Indents as per the requirement.	Web Portal
▪ Receive indents	
▪ Generation of information for press Advertisements	
▪ Check-list for Tender Notice	
▪ Publish Tender Notice	Web Portal
▪ Check-list for Tender Terms & Conditions	
▪ Publish Tender Document	Web Portal
▪ Reports to assist Tender Document preparation	Web Portal
▪ Purchase of Tender Documents	Accounts, Web Portal, CCC
▪ Cross-check of vendors with Vendor Database and their previous records	
▪ Cross-check of rates with similar projects in past	Projects
▪ Award of contract	Projects
C] Procurement via Local Market / through quotations	
▪ Invitation of Quotations	
▪ Issue of Purchase order	
▪ Receipt of Material	Central Stores
▪ Payments	Accounts
D] MIS	
▪ Technical Bid Comparison Reports	
▪ Financial Bid Comparison Reports	
▪ List of Vendors registered	

4. Disaster Recovery

The scope of services shall comprise the following:

- Project Planning & Management
- Design, configuration, installation and setup of DR site
    - Configure solution for specified features
    - Hardware and a Software based solution, with requisite licenses
    - Data replication and application replication
    - 2-way data replication in an asynchronous mode
- Testing Applications on DR site
- Maintenance & Support of DR solution
- Change Management Workshops
- Preparation of Disaster Recovery Plans

In implementing the above, the bidder shall strictly adhere to the standards set by Authority. The details about the above mentioned services are covered in subsequent sections.

4.1. Project Planning & Management

The success of the project depends on the proper project planning and management. At the onset, the Service Provider shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with Authority. An indicative list of planning related documentation that the Service Provider should make at the onset is as follows:

- **Project Schedule:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same
- **Manpower Deployment List:** A list needs to provide with resources who will be deployed on the project along with the roles and responsibilities of each resource.
- **Resource Deployment List:** List and number of all resources (including but not limited to servers, storage, network components and software licenses) other than manpower that may be required.
- **Communication Plan:** Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- **Progress Monitoring Plan:** Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will approved by Authority to the successful bidder before start of the project.
- **Standard Operating Procedures:** Detailed procedures for monitoring the DR site parameter, periodic DR drills and operating procedures to be followed in event of a disaster. The periodic DR drills will be scheduled once every 6 months and will last for one day. During such DR drills all

applications will run from the DR site as drills will be performed after a switchover. Ensuring data synchronization on DC site after drill/ disaster will be DR Service provider's responsibility.

- **Risk Mitigation Plan:** List of all possible risks and methods to mitigate them.
- **Escalation Matrix & Incident Management:** A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.

4.2. Implementation Plan

The service provider should prepare and submit a detailed plan during execution of order with following details:

Mapping of detailed hardware at primary site and DR site should be prepared with detailed analysis including following parameters:

- CPU calculations
- RAM calculations
- Disk calculations

4.3. Network interfaces requirement

- Network throughput requirement
- Backup requirement

Detailed planning of hardware deployment and configuration should be submitted to Authority. The configuration planning should include following details.

- Network architecture planning including
  - VLAN configuration planning
  - IP address planning
  - Subnet planning and routing planning
- Firewall configuration planning
- Backup methodology
- Failover mechanism for replication links

4.4. Roles and Responsibility of Service Provider

The service provider will be responsible for providing a tier 3 or above DR site within India, where Authority applications will be hosted.

- The DR site within India should be at least 150 Km away from the Authority Data Center and in a different seismic zone.
- The service provider shall develop, prepare and provide a DR Implementation Plan. The Implementation Plan shall have the detailed design, specifications, drawings and schedule along with inspection and test plan, risk matrix and risk mitigation strategy, training material and documentation for all deliverables

- Responsible for the replication of data between WDC and the proposed DR site. The service provider will be responsible for commissioning the bandwidth required for replication of data and the SLA for the replication of data will be attributed to the service provider.
- The solution is envisaged for application level recovery scalable to site level recovery based on the impact of the disaster.
- Network setup and uninterrupted availability through a network link dedicated for connecting between the main DC site and DR site
- Perform the Disaster Recovery operation planning exercise for each applications envisaged in this RFP and in the scope of the bidder. Such a Disaster Recovery operations plan must include:
    - Key Processes automated by the application and key process owners
    - Hardware and Software technology stack of application
    - Identification of business activities of the processes including criticality, impact and dependencies
    - Incident response scenarios with accurate stakeholder mapping
- Conduct a requirement analysis and conduct the infrastructure sizing for the DR site
- Prepare a private cloud environment for creating instances of existing applications for DR
- Shared storage sizing for DR requirements
- Test run for all these applications at the DR site
- Necessary support in bringing the machines to login level in case of disaster / DR drills
- Provisioning, configuring and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router
- Regular back up of data at DR site through Asynchronous based replication
- Support during the recovery operations of data from DR site
- Ensuring related DNS changes for private WAN and internet, application availability and integrity, and database synchronization with application at DR site.
- It will be responsibility of the service provider to ensure RTO and RPO by using global load balancing.
- Installation and Supply of any components (including FC-IP routers if required) at primary site to ensure RTO and RPO will be responsibility of the service provider.
- 24x7x365 support for Hardware restoration (from self and OEMs), managed hosting support (including L1, L2, and L3 support), Uptime commitment up to OS levels, managed & monitored backup and backup retention (as per period required by Authority), OS provisioning & management, dedicated security services operations, etc.
- Monitoring and maintenance reports over a monthly basis and as and when required
- Availability of server logs/ records for audits

- Access to monitoring tools for measuring the service levels, application performance, server performance, storage performance and network performance.
- Support in audit of the entire system on an yearly basis
- Preparation of disaster recovery plans and guidelines for Authority providing details of
    - The key persons to be contacted during the disaster
    - The various activities to be done by vendor and Authority for complete operations from DR site and restoration of operations to main DC site
- On expiration / termination of the contract, handover of complete data in the desired format to Authority which can be easily accessible and retrievable
- Compliance process to the defined international security guidelines such as ISO 27001 for maintaining operations of cloud and ensuring privacy of Authority data. For the same an audit will have to be conducted on a periodic basis as per section 5.7.3
- In the event of the disaster, the servers available at the DR site should be at least 100% of the servers for the listed applications at the primary data centre without requirement of fail-over.
- The DR infrastructure and Authority data must be maintained at the location of the identified DR site. Data can only be moved to other site in case of any emergency with prior approval of Authority concerned authority
- Availability of data / application as per the defined RPO (1 hour) / RTO (4 hours) requirements as mentioned in the SLAs
- The bandwidth required for Authority employees to use the applications from the DR site in case of DR drills or in the event of a disaster will be procured by Authority separately. The DR Service provider will be responsible for core infrastructure facility for provisioning of internet, MPLS/ point to point connectivity including termination devices, network security in terms of firewall and IPS. However, the service provider will have to coordinate with the bandwidth provider and offer support to an extent to ensure that applications are accessible across Authority offices.
- Scaling the server and storage infrastructure up or down based on the needs of Authority
- In addition to the DR site, Authority may also plan to have a near DR site solution in future. This will be done to cater to the requirement of no data loss acceptable for highly critical applications. The solution should be scalable to provide 3 - way DR replication in future. The selected vendor should have capability to provide the same, based on Authority's requirement and data centre location.
- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the DR vendor.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Primary DC site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre. Restoration at Primary

Data Centre will be the prime responsibility of FMS vendor, but necessary support has to be provided by the DR Service Provider.

- The backup is required at the DR site, wherein a disaster has happened and DR site is acting as DC site. The backup is not limited using tape drives only, however bidder need to provide solution taking backup for the duration in case DR is acting as main operations site. Daily incremental and weekly full backup needs to be taken when the DR is functioning as DC. Backup is not expected when DR is not active.
- It will be the Service Provider's responsibility to ensure that back up data is in a format that is restorable at Primary Data Centre.
- In case Authority augments or updates the infrastructure, operating system or system software the DR provider will have to update the disaster recovery site accordingly in order to ensure business continuity. The updates to such infrastructure will be made through equivalent price discovery components.

4.5. Testing

Testing Planning

Following hardware deployment, the testing of application at DR site becomes very important. Therefore the service provider must perform following testing:

- Infrastructure testing - The bidder should perform various testing procedures listed below on infrastructure (server, storage and network infrastructure) provided at DR site.
    - Disk IO testing.
    - Network throughput testing
    - CPU and RAM benchmarking testing
    - Read/Write latency testing
- Application Testing - Once system is exported, data is migrated to DR site and application starts to function, the functional testing of application will be done by service provider. The service provider will have to seek inputs from Authority and the application vendor for the same.
    - Software Module testing up to the login screen of application
    - Heavy application transactions on DR servers including performance of application to be benchmarked against data centre performance.
    - Backup exports
    - Backup restoration
    - Performance Testing of Application
- Data Integrity Testing - Data integrations will be very important factor in overall process. Since data will be replicated over any platform including same database at both end, the data integrity testing would become crucial. Data integrity testing will be performed by service provider and this includes:
    - Table size and records testing

- Transactions verification at DR and DC site
- Data in log files

❖ Reverse Replication testing - The reverse replication from DR side to DC site needs to be verified by service provider. The testing should include the:

- Uninterrupted replication to DC servers.
- Lag in replication due to any unforeseen errors.
- Process of recovering from lags if any.
- Data integrity test of DC servers.
- Switch over of applications from DC to DR
- Switch back of applications from DR to DC

❖ Switch Over testing – The final operation acceptance will only be provided after demonstrating successful switchover testing for each of the project phases identified. The switchover testing would include:

- Switch over of application from DC to DR as per defined RTO and RPO
- Switch over applications from DR to DC as predefined RTO and RPO
- Complete Data Replication and Reverse Data Replication as per RPO

Service Maintenance

Service provider must maintain the infrastructure at DR site. If any system has to be upgraded at DR end, that should be done by the bidder.

- Monitoring of Replication status.
- Lag in replication due to any unforeseen errors.
- Network monitoring
- Security monitoring and analysis
- Reporting if any issue is arising in replication.
- Daily backup at DR end.

4.6. Preparation of Disaster Recovery Operational Plan

- The bidder should provide detailed operating procedures for each application during the following scenarios. These will be mutually agreed upon with Authority during the project kick off.
  - Business as usual: the primary site is functioning as required, procedures for ensuring consistency of data availability at secondary site.
  - Disaster: Declaration of disaster, making the DR site live for production, ensuring availability of users to the secondary site.
  - Operations from DR site: Ensuring secondary site is addressing the functionality as desired

- Restoration to Normalcy: Reverse replication of data from DR site to primary site, ensuring availability of users to the primary site.

4.7. Configure proposed solution for usage

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

#	Features
1	The proposed solution must offer a workflow based management& monitoring and reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts(including SMS and e-mail alerts) on any deviations. The proposed solution should be able to conduct DR Drills from a centralized location
2	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR
3	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness
4	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions
5	The proposed solution should facilitate out-of-the-box, workflow based switchover and switchback for DR drills for standard applications based on industry best practices
6	The proposed solution should facilitate workflows for bringing up the applications and all the components it depends on at DR while it is up at primary site without pausing/stopping the replication
7	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should not require any change in the existing environment
8	The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms
9	The proposed solution should facilitate workflow based, single-click recovery mechanism for single or multiple applications
10	The proposed DRM solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters
11	The proposed solution should cover all the functionalities mentioned in the specifications and all the required licenses should be provisioned

4.8. Periodic Disaster Recovery Plan Update

The service provider shall be responsible for –

1. Devising and documenting the DR policy discussed and approved by Authority.
2. Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.

5. Generalized Scope of work

From the perspective of project implementation, the scope has been categorised as follows:

A) Implementation Services

- Assess and Prepare for each phase
- Implement in each phase

B) Post-Implementation Services

- Maintenance of each phase along with Helpdesk and facility management services

5.1. Prepare & Access

Finalise the camera distribution and exact locations of the cameras at different junctions in consultation with Authority

Bidders are required to note that while executing the Project, the Successful Bidder shall prepare the final camera distribution plan at all the camera locations in discussion with Authority. Actual location for placement of pole & number of cameras at each location, type of cameras, fixation of height & angle for the cameras would be done carefully to ensure optimum coverage. Based on the site survey, there could be some variation in types/number of the cameras at certain locations compared to the indicative site list given in this Tender. Payments to be made to the Systems Integrator shall also be based on actual number of cameras and type of cameras installed and unit rates quoted by the Successful Bidder shall be used to arrive at the same.

Finalise the Bill of Material for the number and type of the cameras to be implemented

The bidder shall prepare the detail report on Edge level requirements – cameras (types & numbers), camera mounting requirements, power requirements, and connectivity requirements. Indicative list of the edge level hardware / services is as follows:

- Cameras (Fixed Box Cameras, PTZ Cameras)
- IR Illuminators
- Managed switches
- Junction boxes
- Pole/ Mast
- Digging & trenching
- Networking cables and other related infrastructure
- Provisioning of electrical power/backup

During the course of the project, if some camera requires change of field of value, it should be done by SI without any extra cost, in consultation with Authority/Authority. However, number of such instances would be kept in check and are expected to be rare. Successful Bidder is expected to accommodate such efforts in the regular post implementation support.

Finalisation and submission of a detailed technical architecture and submission of a detailed project plan

Within 1 week of the work order, the Systems Integrator needs to deploy the team proposed for the Project and ensure that a Project inception report (phase I –deliverable) is submitted to Authority which should cover following aspects:

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

Thereafter, within 2 weeks from submission of inception report, SI shall submit the detailed Technical Architecture, which should take into consideration following guiding principles:

- **Scalability** - Important technical components of the architecture must support scalability to provide continuous growth to meet the growing demand of Authority. 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 or other edge devices. Main technology components requiring scalability are storage, bandwidth, computing performance (IT Infrastructure), Software/application performance and advancement in camera features. In quantitative terms, there may not be major change in number of Command and Communications Centers.
- **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 Bidder 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.
- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. Successful Bidder 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 endeavor 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. Authority would carry out the security audit of the entire system in approx. 3 months of Acceptance / operationalization through a Third Party Auditor (TPA). The following guidelines need to be observed for security:
    - Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
    - The most appropriate level of security commensurate with the value to that function for which it is deployed must be chosen

- Access Controls must be provided to ensure that the system is not tampered or modified by the system operators or unauthorized persons.

- Implement data security to allow for changes in technology and business needs.

Field equipment installed through this Project would become an important public asset. During the implementation phase of the Project the SI shall be required to repair / replace any equipment if stolen/damaged. Appropriate insurance cover must be provided to all such field equipment.

- **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.

- **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. Also system should have integration capabilities between various IT systems of the Authority as indicated in scope of work. The system can integrate with social media platforms for social media monitoring. It may be noted that most of the systems deployed by these large private / public/community establishments use open standards. Bidder may carry out further study on the same. Authority shall facilitate to get cooperation from the private / public establishments for community monitoring.

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

- Passive networking & civil work during implementation,

- Viewing manpower at Command / viewing centers & Mobile Vans during post-implementation

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

- Services of professional architect for design of command / viewing centers

Sub-contracting / outsourcing shall be allowed for each such need as mentioned in the clause with prior written approval from Authority. However, even if the work is sub-contracted / outsourced, the sole responsibility of the work shall lie with the Bidder. The Bidder shall be held responsible for any delay/error/non-compliance 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 Authority.

Finalise the detailed Technical Architecture for the network

The Successful Bidder will be required to review the Technical Architecture suggested in the Tender and finalize the detailed architecture for the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time video stream to the Command Centers and viewing centers, Tablets for select officials through Data Centers. All the components of the Technical Architecture should be of leading industry standards.

Design the LAN connectivity requirements at locations

The Successful Bidder shall be responsible for gathering the LAN connectivity requirements at junctions, Data Centers, Command Centers, and viewing centers. The LAN connectivity may involve setting up the structured cabling, commissioning of active and passive components for operationalization of the Surveillance System. The core (backbone) network connectivity is out of Bidder's scope (to be provided by APSFL), last mile connectivity i.e from junction aggregation points to edge devices, is to be provided by the Bidder. The details of the core connectivity will be shared with the Successful Bidder.

With advancement of technology, if at the same bandwidth higher resolution can be transmitted, the same shall be adopted. SI shall make available such technological benefits to Authority within 120 days of when

such advancements are made available in the open market. If such advancements are available without any additional cost impact to the SI, these would be made available to Authority without any extra cost.

The actual bandwidth requirement and storage parameters required to meet SLAs should be calculated by the Bidder and the same shall be clearly proposed in the Technical Bid with detailed calculations. Authority also requires the Bidder to meet the parameters of video feed quality; security & performance and bidders should factor the same while designing the solution.

Bidders are also required to estimate the bandwidth requirement for other connectivity (between Data Centers, Command Centers / viewing centers at Zonal Offices etc.) and propose in the Technical Bid.

Finalise the Bill of Material for the Data Center Infrastructure

As part of preparing the final bill of material for the physical Data Centers, the Successful Bidder will be required to list all passive & active components required in the Data Centers. The bill of material proposed by the Successful Bidder will be approved by Authority for its supply and installation. Indicative equipment to be commissioned as part of Server Side infrastructure at Data Centers is as under:

- Servers (inclusive of OS)
    - Application Servers
    - Recording Server
    - Analytics Server
    - Database Server
    - Management Server
    - Enterprise Backup Server
    - Domain Controller
    - Antivirus Server
    - Server Load Balancer
    - Any other Server required to cater to the scope of work mentioned in this Tender volume
- Application & system software
    - Video Management System
    - Updated Base Map of Hyderabad City (Min 1:1000)
    - Viewing Software for GIS
    - Backup Solution
    - Enterprise Management System including SLA Management, Helpdesk Management, Network Management & BMS
    - Anti-virus Software
    - LDAP Software

- Custom Software as needed to fill gaps, from open commercial market , to cater to the Project requirements
- ANPR (Software & License)

- Workstation for Administrative Staff
- Storage and storage management solution
- Tape Library (as per requirement)
- Core Router
- Switches (L2 & L3 Switches)
- Firewall
- Intrusion Prevention System
- Racks (Caged from all sides except data center floor)
- Indoor Fixed Dome Cameras
- Fire Proof Enclosure for Media Storage
- All required Passive Components
- Data Backup Solution

The above are only indicative requirements of IT and Non-IT Infrastructure requirements at Data Centers. The Bidder may propose virtualization. The exact quantity and requirement would emerge after the Project Design Document, prepared by the Successful Bidder and is approved by Authority. Benchmark specifications for various items mentioned above are given in the Annexures to this Tender Document.

Note: As part of the scope of work of this Tender, the Successful Bidder shall build the Data Center as per the defined requirement. However Authority reserves the right to go for Co-Location of Data Center. The decision of Authority will be final in this regard. In such case, the payment milestones, Service Level Agreement and roles and responsibilities, shall be revised accordingly.

Prepare roll-out plan for deployment & operationalisation of equipment

The Successful Bidder shall prepare the overall Data Center establishment & their operational plan for this Project. The plan shall comprise deployment of all the equipment required under the Project. The implementation roll-out plan for setting up the Data Center shall be approved by Authority. The detailed plan shall also comprise of the scalability, expandability and security that the Data Center will implement under this Project.

Preparation of Detailed FRD, SRD and SDD for the Surveillance System and for integration with other systems

The present RFP covers the key expectations from the Project and various scope elements. However, it is required that the Successful Bidder documents the requirements in detail before the work on execution begins. Following documents are expected to be delivered as part of this documentation:

- **Functional Requirements Documentation**, giving complete details of the functional aspects of the Project. Some of the key functional requirements for designing the system are given in Annexure 2.

- **System Requirements Documentation**, giving complete details of the entire system components and their inter relationships to execute the Project once operational

- **System Design Documentation**, detailing out the design of the Surveillance System, Command & Communications Centers in particular, including integration with various IT enabled systems like Vehicle Tracking, e-Challan system, CCTNS, Community Surveillance, etc. currently available or being implemented by Authority. The document should also detail out the social media monitoring and integration with social media platforms.

The Successful Bidder shall prepare above mentioned documents in discussion with all key stakeholders (Client, Project Management Consultants, and Project Management Unit). It is expected that the Successful Bidder brings in leading international best practices in this field and ensures that a progressive system is implemented for the IP based Citywide CCTV Surveillance System for Authority.

GIS Integration

System Integrator shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras, GPS fitted police vehicles (Vehicle Tracking) are brought out on the GIS map. SI is required to carry out the seamless integration to ensure ease of use of GIS in the Surveillance System Applications/Dashboards in Command & Communications Centers, Zonal offices, & by other authorized senior officials. GIS Base Map shall be developed or procured, supplied and integrated by the Systems Integrator at 1:1000 scale or better with all surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. If this requires field survey, it needs to be done by Successful Bidder. If such a data is already available with Authority shall facilitate to provide the same. Bidder is to check the availability of such data and it's suitability for the project.SI is required to update GIS maps from time to time. Different layers to be covered under GIS are as follows:

- Cameras and areas covered by camera field of view

- Buildings/Structures

- Roads

Geographical coverage of the Project is under the jurisdiction of Authority. SI shall supply viewing software for GIS Maps and shall ensure that GIS application is integrated with VMS to support the Command Centers / Authority to navigate on the map and use it for better spatial understanding. It should also help higher management of Authority to analyses the events on a spatial perspective.

GPS integration with GIS is required to locate all police vehicles (on which GPS units are fitted) on GIS Map. Vehicle tracking should happen even while any vehicle is parked/stationary/ignition-off.

SMS Gateway Integration

SI shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass SMSs to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation.

Detailed assessment of infrastructure requirements at Command & Communications/Control Centers

Command & Communications Centers would be equipped with state of the art equipment to support monitoring and analysis of video feeds.

The Command & Communications/Control Centers will also have a room identified for IT Analytics and Forensic Experts where they will analyze the incriminating video footage and certify its integrity & chain

of custody. These experts shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyze various analytics related technologies and their implementation over the years. SI shall engage services of a professional architect to prepare appropriate design layout at the location finalised by Authority.

Finalise the Bill of Material for Command & Communications/Control Center

Broad level Bill of Material for IT Infrastructure at different command/viewing centers is given below:

Command & Communications Centers

- **IT Components**
    - Video Wall
    - Monitoring Workstations (Computers)
    - Additional Displays (Full HD viewing capacity)
    - Network Color Laser Printers
    - Indoor Fixed Dome Cameras for Internal Surveillance
    - Active Networking Components (Switches, Routers)
    - Passive Networking Components
- **Non-IT Components**
    - Electrical Cabling and Necessary Illumination Devices

Fire Safety System with Alarm

- Access Control System (RFID/ Proximity based, for all staff)
- Full Biometric System to control entry / exit
- Office Workstations (Furniture and Fixtures)
- Comfort AC
- UPS (1 hour backup)

Automatic DG set to provide power backup for 12 hours to the Command & Communications Center

Viewing centers as decided by authority

Broad level Bill of Material required is as follows:

IT Components

LED Displays (Full HD viewing capacity)

Monitoring Workstation (Computers)

Switches / Routers

Non-IT Components

Office Workstations (Furniture and Fixtures)

UPS (30 minutes backup)

Plan to integrate the Community Surveillance

Surveillance cameras have been planned to be deployed at various community areas within Authority limits. The prime monitoring of community cameras will be done. As the community cameras are at located at sensitive areas hence it is important that these cameras are integrated as a part of the new Surveillance System.

VMS should have provision to ensure that such video feeds can be streamed to the Command & Communications Centers and if required to Zonal viewing centers too.

5.2. Supply, install, commission & configure cameras

The Successful Bidder will be required to supply, install, configure and integrate the surveillance cameras at the identified locations and then undertake necessary work towards their commissioning. The Successful Bidder will also be commissioning the surveillance cameras required in the Mobile Vans.

SI should use the industry best practices while positioning and mounting the cameras. Some of the check-points which need to be adhered by the SI while installing / commissioning cameras are as follows:

- Ensure Project objectives are met while positioning the cameras, creating the required field of view
- Ensure appropriate housing is provided to protect camera from the on field challenges
- Carry out proper adjustments to have the best possible image
- Ensure that the pole / mast implementation is vibration resistant
- During implementation period, in case any camera is damaged by a vehicular accident (or due to any other reason outside the control of SI) and needs repair, then the SI will need to repair / have the new camera within 15 days of the incidence. Damages are to be borne by SIs in such cases through proper insurance.

Obtain all necessary legal/statutory clearances for erecting poles

Successful Bidder will have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras, for provisioning of the required power, etc. It is important to mention that a timely communication and required follow-up will be required by the Successful Bidder for the clearances.

Authority shall extend necessary support to the Successful Bidder (in terms of documentations, meetings with concerned authorities, etc.) for getting the approvals from concerned authorities, if all the necessary requirements are in place. It would be responsibility of Successful Bidder to obtain these permissions from concerned authorities. All the possible support in expediting such permissions would be provided from the Authority. Delay caused due to any reason not in control of the Successful Bidder would be considered appropriately for the project timelines.

SI will have to then supply & erect poles at these locations well in advance to meet the camera installation timelines.

During implementation period, in case the pole is damaged by a vehicular accident (or due to any other reason outside the control of SI) and needs repair, then the SI will need to repair / have the new pole within 15 days of the incident. Damages are to be borne by SIs in such cases through proper insurance.

Provision of the Electricity

For the successful commissioning & operationalisation of the edge devices and to provide the video feeds to Command & Communications Centers and the Successful Bidder will be required to provide electricity to the edge devices through the aggregation points. Bidder has to plan the power backup based upon the power situation across the city.

Since this component has dependency on approval from other agencies, it is recommended that SI plans this requirement well in advance & submits the application to the concerned electricity distribution agency. Registration of electrical connections is to be done in the name of Authority. The SI has to carry out study and identify locations to provide UPS backup, depending upon power situation across city, so as to meet the camera uptime requirements. Authority shall extend necessary support to the Successful Bidder (support in terms of documentations, meetings with concerned authorities, etc.) for getting the approvals from concerned authorities, if all the necessary requirements from the Successful Bidder are in place.

Deploy / Develop, Test and Commission the Surveillance System

The Successful Bidder will be responsible for the solution deployment / customisation for implementing end-to-end Surveillance System including its integration with other systems as mentioned above. The application will be customised to meet the Project objectives and the requirements of Authority. The Bidder will ensure that the best practices for software development and customisation are used during the software development/customisation and implementation exercise. This would at a minimum include:

(a) Software development/customisation based on the functional requirement specifications, system requirement specifications, software requirement specifications and solution designs as finalised and approved by the Authority. Wherever necessary, the Successful Bidder shall develop additional functionality/modules on top of COTS products, in order to meet the Project requirements.

(b) Delivering the Surveillance System, along with all of the necessary modules and additional functionalities/ integrated products, utilities, system drivers and documentation consistent with proven standards, including product updates, technology upgrades and patches to run on the selected operating system(s) and hardware according to the solution.

(c) Deployment and commissioning of Surveillance System with all the necessary solution elements at the Data Center. It is pertinent to mention that application hosted at the Data Center shall be accessible by the intended users as desired under this Project.

(d) Provision for Authority officers to login into the system remotely from any location via a secure private network.

Supply, Install & Configure all the User Level components (Active & Passive) at Command & Communications Center

The System Integrator shall develop a plan to procure, install, and configure all the necessary items for the Command & Communications Centers, viewing centers in a timely fashion in different phases. There should be a tracker created and shared with Authority that would track all the commissioning of the equipment, the timelines adhered to and the compliance to the requirements.

Supply, install, configure & commission Server Side Infrastructure

The Successful Bidder shall provide system integration services to procure and commission the required software and hardware infrastructure at the Data Centers and deploy the complete surveillance management applications. The SI shall be completely responsible for the sourcing, installation, commissioning, testing and certification of the necessary software licenses and infrastructure required to deploy the solution at the Data Centers. The SI shall be responsible for provisioning of connectivity from cameras to Data Centers and Data Centers to the Command and Control Centers.

The System Integrator shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the Project to verify the actual quantity of the equipment supplied and commissioned under the Project.

Partial Acceptance Testing & Final Acceptance Testing of Project phase wise

The acceptance test for the Project shall be carried as per the phases by the Authority or any duly appointed Independent Evaluation Agency by Authority. The Successful Bidder should cooperate with the IEA to ensure successful completion of acceptance tests.

The acceptance test shall consist of a Partial Acceptance Test (PAT) and Final acceptance test (FAT) for Phase I. For remaining phases the FAT shall be issued after PAT of the respective phase along with integration of the scope of work for earlier phases.

The SI shall submit a detailed acceptance testing document at the stage of planning and Authority & the Successful Bidder shall mutually agree upon the same.

Partial Acceptance Test

Partial Acceptance Test shall involve scrutiny of documents for various IT / Non-IT components to verify if the specifications conform to the technical and functional requirements mentioned in the Tender and subsequent corrigendum. Authority reserves right to conduct physical inspection of the equipment delivered to ensure that they arrive at the sites in good condition and are free from physical damage and incomplete shipments and shall return the products to the supplier at the supplier's expenses if required quality is not maintained. Physical inspection of hardware will also include physical checking and counting of the delivered equipment in presence of the Successful Bidder. This equipment will only be acceptable as correct when each received item corresponds with the checklist that will be prepared by the SI prior to shipment. Any shortfalls in terms of number of items received may render the delivered equipment incomplete. SI shall submit TPA test reports on performance for the critical components like cameras, active network equipment's, servers, video wall, etc. The TPA should be approved by police department. Physical verification of the individual items would be undertaken as part of FAT for Server Side equipment.

Final Acceptance Test

After successful installation of equipment in accordance with the requirements in the Tender, the Successful Bidder would need to carry out Final Acceptance Testing in 2 different phases - (a) Unit Testing and (b) Integration Testing. These tests would be carried out based on the test cases developed and

validated by Authority. Apart from the functional testing of the entire system components, the testing would also verify following aspects:

- Configuration Testing (to ensure that all the components are configured properly)
- Security Testing (to review & evaluate security controls)

Final acceptance certificate shall be issued by Authority to the Successful Bidder after successful testing in a real time condition for at least 15 days of trouble free operation. The date on which final acceptance certificate is issued for final phase shall be deemed date of the successful commissioning of the Project. Authority shall consider implementation of 95 percent cameras of the phase as a sufficient condition for the overall Project Go-Live for that phase. Any delay by the Successful Bidder in the performance of its contracted obligations shall render the Successful Bidder liable to the imposition of appropriate liquidated damages or termination, unless agreed otherwise by Authority.

System Documents, User Documents

The Successful Bidder will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the Project undergoes various stages of implementation. Indicative list of documents include:

- **Project Commencement Documentation**: Project Plan in giving out micro level activities with milestones & deadlines.
- **Cabling Layout:** Systems Integrator shall submit the detailed cabling layout including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways.
- **Equipment Manuals**: Original Manuals from OEMs.
- **Installation Manual**: For all the application systems
- **Training Material**: Training Material will include the presentations used for trainings and also the required relevant documents for the topics being covered. Training registers should be submitted for same.
- **User Manuals**: For all the application software modules, required for operationalisation of the system.
- **System Manual:** For all the application software modules, covering detail information required for its administration.
- **Standard Operational Procedure (SOP) Manual**: The Bidder shall be responsible for preparing SOP Manual relating to operation and maintenance of each and every service as mentioned in this Tender. The draft process (SOP) document shall be formally signed off by Authority before completion of Final Acceptance Test. This SOP manual will be finalised by the Bidder within 2 months of operationalisation of each phase, in consultation with the Authority and formally signed off by the Authority.

Note: The Successful Bidder will ensure upkeep & updation of all documentation and manuals during the contractual period. The ownership of all documents, supplied by the Successful Bidder, will be with Authority. Documents shall be submitted in two copies each in printed (duly hard bound) & in softcopy formats.

Post Implementation Services

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the Systems Integrator perspective too this is a critical phase since

the quarterly payments are linked to the SLA's in the post implementation phases. System Integrator thus is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs.

Helpdesk and Facilities Management Services

The Successful Bidder will be required to establish the helpdesk and provide facilities management services to support the Authority officials in performing their day-to-day functions related to this system.

The Successful Bidder shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by their field units, proposed to be setup at Command & Communications Centers and various Viewing Centers. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted. Central Helpdesk can be set up at any of Command and Control Centers.

Functional requirements of the helpdesk management system, fully integrated with the enterprise monitoring and network management system. The system will be accessed by the Authority officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the Successful Bidder is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender. Systems Integrator is also required to depute a dedicated, centralised project management & technical team for the overall Project management and interaction with Sr. Police Dept. personnel. Indicative resource requirement for this centralised administration of the Project is as follows:

Provision of the Operational Manpower to view the feeds at Command and & Communications Centers

Authority may ask the System Integrator to provide suitable manpower to monitor the feeds at Command and Communications Centers and support Authority in operationalisation of the Command and Communications Centers. The exact role of these personnel and their responsibilities would be defined and monitored by Authority personnel. System Integrator shall be required to provide such manpower meeting following requirements:

- All such manpower shall be minimum graduate pass
- All such manpower shall be without any criminal background / record.
- Authority reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
- System Integrator shall have to replace any person, if not found suitable for the job.

All the manpower shall have to undergo training from the System Integrator for at least 15 working days on the working of Command and Communications Centers. Training should also cover dos & don'ts and will have few.

- Sessions from Authority officers on right approaches for monitoring the feeds & providing feedback to Police Personnel / Surveillance System.
- Each person shall have to undergo compulsory 1 day training every month
- Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.

Authority reserves the right to include or exclude this scope of providing operational manpower in the Project scope or include it partly at the time of signing of the contract or during execution of the contract. Current estimation of the man-power required from the SI for viewing of the feeds is as follows:

6. Functional & Technical Specifications

6.1. Command and Communications Center (CCC)

6.1.1. Objectives

1) The vision of the Command and Communications Center (CCC) is to have an integrated view of all the smart initiatives undertaken by Authority with the focus to serve as a decision support engine for city administrators in day-to-day operations or during exigency situations. This dynamic response to situations, both pre-active and re-active will truly make the city operations "SMART".

2) Command and Communications Center (CCC) involves leveraging on the information provided by various departments and providing a comprehensive response mechanism for the day-to-day challenges across the city. CCC shall be a fully integrated, web-based solution that provides seamless incident – response management, collaboration and geo-spatial display.

3) 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 smart city operations center shall be accessible by operators and concerned authorized entities with necessary authentication credentials.

4) 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) Command & Communications Center should be able to integrate with various Utility systems such as Water/SCADA, Power, Gas, ITMS, Sewerage/ Drainage system, Disaster Mgmt. System etc.

6.1.2. Proposed Components of CCC Solution

- Event Management System
- Flood / Tsunami / Cyclones Modelling System
- Incident Management System
- Alerting System
- Unified Communications & Contact Center
- Radio & Communication Systems
- Video Display System
- Structured Cabling System
- Social Media System
- Logging Solution for Voice, Video & Radio

6.1.3. Functional Specifications of the Application Software

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

#	Functions	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.
2.		Must have built-in fault tolerance, load balancing and high availability & must be certified by the OEM.
3.		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.

#	Functions	Minimum Specifications
4.		System must provide a comprehensive API (Application Programming Interface) or SDK (Software Development Kit) to allow interfacing and integration with existing systems.
5.		The solution should be network and protocol agonistic and provide option to connect legacy system through APIs with either read, write or both options. It should connect diverse on premise and/or cloud platforms and makes it easy to exchange data and services between them.
6.		The system shall allow seamless integration with all of the department's existing and future initiatives (e.g. open source intelligence, situation management war room, etc.)
7.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used.
8.		The platform should be able to normalize the data coming from different devices of same type (i.e. different lighting sensors from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers
9.	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 have capability to source data from various systems implemented in Vizag (being implemented as part of this project or other projects) to create actionable intelligence
10.	Industry Standards for the Command and Communications Center	The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility
11.		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management
12.		Geo Spatial Standards like GML & KML etc.
13.		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
14.	Command and Communications 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.

#	Functions	Minimum Specifications
15.		**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. Analytics functionality can be part of application server or separate server
16.	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:
17.		Should support comprehensive reporting on event status in real time manually or automatically by a sensor/CCTV video feeds.
18.		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention.
19.		Should support for multiple incidents with both segregated and/or overlapping management and response teams.
20.		Should support Geospatial rendering of event and incident information.
21.		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.
22.		Should support incorporation of resource database for mobilizing the resources for response.
23.		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.
24.		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems
25.		Should provide detailed reports and summary views to multiple users based on their roles.
26.		A Reference Section in the tool must be provided for posting, updating and disseminating plans, procedures, checklists and other related information.
27.		Provide User-defined forms as well as Standard Incident Command Forms for incident management.

#	Functions	Minimum Specifications
28.	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
29.		• 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.).
30.		Should provide tools to assemble personalized dashboard views of information pertinent to incidents, emergencies & operations of command center
31.		Should provide historical reports, event data & activity log. The reports can be exported to PDF or HTML formats.
32.		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
33.	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.
34.		Should extract messages and display it in an operational dashboard.
35.		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.
36.		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.
37.		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.
38.	Device Status, Obstruction Detection and Availability Notification	Should provide ICON based user interface on the GIS map to report non-functional device.
39.		Should also provide a single tabular view to list all devices along with their availability status in real time.
40.		Should provide User Interface to publish messages to multiple devices at the same time.

#	Functions	Minimum Specifications
41.	Event Correlation	Command and Communications 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.
42.	Standard Operations Procedures (SOP)	Command and Communications Center should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
43.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.
44.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.
45.		The users should be able to also add comments to or stop the SOP (prior to completion).
46.		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.
47.		The SOP Tool should have capability to define the following activity types:
48.		**Manual Activity** - An activity that is done manually by the owner and provide details in the description field.
49.		**Automation Activity** - An activity that initiates and tracks a particular work order and select a predefined work order from the list.
50.		**If-Then-Else Activity** - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
51.		**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.
52.		**SOP Activity** - An activity that launches another standard operating procedure.
53.	Key Performance Indicator	Command and Communications Center should be able to facilitate measurement or criteria to assay the condition or performance of departmental processes & policies.
54.		**Green** indicates that the status is acceptable, based on the parameters for that KPI, no action is required.
55.		**Yellow** indicates that caution or monitoring is required, action may be required.
56.		**Red** indicates that the status is critical and action is recommended.

#	Functions	Minimum Specifications
57.	Reporting Requirements	Command and Communications 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
58.		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
59.	Collaboration Tools	Should provide tools for users to collaborate & communicate in real-time using instant messaging features.
60.	Communication Requirements	The solution should adhere to the below mentioned communication requirements.
61.		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
62.		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.
63.		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
64.		The solution should provide Dispatch Console integration 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.
65.	Authentication	Use authentication information to authenticate individuals and/or assign roles.
66.	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.
67.	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command and Communications 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 and Communications Center, the event should be displayed on an operations dashboard and analyzed to determine a proper directive.

#	Functions	Minimum Specifications
68.		Directives issued by the Command and Communications 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.
69.	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.
70.		To take proactive decisions that help minimize risks and damages, the solution should provide Analytical and Simulation systems 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.
71.	Alert & Mass Notification Requirements	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.
72.		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
73.		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.
74.	Security & Access Control	Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.
75.	Internet Security	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
76.	Authorization	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.

#	Functions	Minimum Specifications
77.	User group	Should provide 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
78.	Provide multi-dimensional access control	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.
79.	Flexible single sign-on (SSO)	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
80.	Authentication	Support LDAP authentication mechanism
81.	Rule Engine & Optimization	Should have ability to respond to real-time data with intelligent & automated decisions
82.		Should provide an environment for designing, developing, and deploying business rule applications and event applications.
83.		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make
84.		Should have at-least two complementary decision management strategies: business rules and event rules.
85.		Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships

6.1.4. 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, Utility/Surveillance System, GIS Services and Other Services of Authority 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.
   - Access information of water management resources
   - 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 (adaptive 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 to trauma centres in the vicinity to prepare for increased number of emergency care patients.

6.1.5. Other Requirements

1) The Command and Communications 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 network of services in Vizag 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. Authority takes the responsibility of necessary civil work including furniture.

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

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

5) **Security:** Under no circumstances the data accumulated and processed by Command and Control should be compromised. Hence, provisions will be made to keep all the data stored in the platform that is highly secured with required security framework implementation. The platform will be hosted in Data center at a location decided by Authority to be provided by successful bidder. Further the platform will provide an open standards based Integration Bus with API Management, providing full API lifecycle management with governance and security.

6.1.6. Technical Specifications for the hardware components

1. Video Wall Screen

The Video Wall for CCC shall be configured with 3x2 formation of the following Professional Display (TV) Screens:

#	Parameter	Minimum Specifications
2	Screen Size	55" or higher
3	Resolution	Full high definition (1080p) 16:9 Widescreen
4	Contrast ratio	5000:1

#	Parameter	Minimum Specifications
5	Brightness	350 nit
6	Viewing angle	178 degree/178 degree (H/V)
7	Response time	8ms
8	Input	HDMI
9	Control	- On Screen Display (OSD) - IR remote control
10	Operations	24 x 7

2. Video Wall Controller

#	Parameter	Minimum Specifications
1	Controller	. Controller to control Video wall in a matrix as per requirement along with software
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 64-bit Operating System Windows / Linux / Equivalent, with recovery disc
5	RAM	. 16 GB DDR3 ECC RAM
6	HDD	. 2x500 GB 7200 RPM HDD (Configured in RAID 0)
7	Networking	. Dual-port Gigabit Ethernet Controller with RJ-45 ports
8	RAID	. RAID 0, 1, 5, 10 support
9	Power Supply	. (1+1) Redundant hot swappable
11	Input/ Output support	0. DVI/HDMI/USB/ LAN/ VGA/SATA port
12	Accessories	1. 104 key Keyboard and Optical USB mouse
13	USB Ports	2. Minimum 4 USB Ports
14	Redundancy support	3. Power Supply, HDD, LAN port & Controller
15	Scalability	4. Display multiple source windows in any size, anywhere on the wall
16	Control functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate
17	Inputs	To connect to minimum 2 sources through HDMI
18	Output	To connect to minimum 16 Displays through HDMI
19	Operating Temperature	10°C to 35°C, 80 % humidity
20	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with LED Display units

3. Video Wall Management Software

#	Parameter	Minimum Specifications
1	15. Display & Scaling	16. Display multiple sources anywhere on display up to any size

#	Parameter	Minimum Specifications
2	17. Input Management	18. All input sources can be displayed on the video wall in freely resizable and movable windows
3	19. Scenarios management	20. Save and load desktop layouts from local or remote machines
4	21. Layout Management	22. Support all layout from input sources, Internet Explorer, desktop and remote desktop application
5	23. Multi View Option	24. Multiple view of portions or regions of Desktop, multiple application can view from single desktop
6	25. Other features	26. SMTP support
7		27. Remote Control over LAN
8		28. Alarm management
9		29. Remote management
10		30. Multiple concurrent client
11		31. KVM support
12	32. Cube Management	33. Cube Health Monitoring
13		34. Pop-Up Alert Service
14		35. Graphical User Interface

4. Monitoring Workstations

#	Parameter	Minimum Specifications
1.	Processor	Latest generation 64bit X86 Quad core processor(3Ghz) or better
2.	Chipset	Latest series 64bit Chipset
3.	Motherboard	OEM Motherboard
4.	RAM	Minimum 8 GB DDR3 ECC Memory @ 1600 Mhz. Slots should be free for future upgrade. Minimum 4 DIMM slots, supporting up to 32GB ECC
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	Minimum 6 USB ports (out of that 2 in front)
11.	Keyboard	104 keys minimum OEM keyboard
12.	Mouse	2 button optical scroll mouse (USB)
13.	PTZ joystick controller *(with 2 of the workstations in CCC)*	• PTZ speed dome control for IP cameras • Minimum 10 programmable buttons • Multi-camera operations • Compatible with all the camera models offered in the solution • Compatible with VMS /Monitoring software offered

#	Parameter	Minimum Specifications
14.	Monitor	22" TFT LED monitor, Minimum 1920 x1080 resolution, 5 ms or better response time, TCO 05 (or higher) certified
15.	Certification	Energy star 5.0/BEE star certified
16.	Operating System	64 bit pre-loaded OS with recovery disc
17.	Security	BIOS controlled electro-mechanical internal chassis lock for the system.
18.	Antivirus feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
19.	Power supply	SMPS; Minimum 400-watt Continuous Power Supply with Full ranging input and APFC. Power supply should be 90% efficient with EPEAT Gold certification for the system.

5. IP Phone Specifications

#	Parameter	Minimum Specifications
1.	Display	2 line or more, Monochrome display for viewing features like messages, directory etc.
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.	Head set	Port for Head set (Headset also to be provided)
5.	VoIP Protocol	SIP V2
6.	PoE	IEEE 802.3af or better
7.	Supported Protocols	SNMP, DHCP, DNS
8.	Codecs	G.711, G.722 including handset and speakerphone
9.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/ off button, microphone mute
10.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer
11.	Phonebook/Address book	Minimum 100 contacts
12.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)
13.	Clock	Time and Date on display
14.	Ringer	Selectable Ringer tone
15.	Directory Access	LDAP standard directory

IP PBX to support minimum 500 IP Phones with at least 100 concurrent sessions with features like –

- Provide reports for calls based on records, calls on a user basis, calls through gateways etc.
- Able to add bulk add, delete, and update operations for devices and users

- Session Initiation Protocol (SIP) Trunk support
- Centralized, configuration database, Web based management
- Lightweight Directory Access Protocol (LDAP) directory interface
- Facilities to users like Call Back, Call Forward, Directory Dial, Last number Redial, etc.
- Calling Line Identification

6. Desktop

Sr No	Item	Minimum Specifications	Bidder's offer
1.	Make	Must be specified	
2.	Model	Must be specified	
3.	Processor	Intel Core i5-latest generation (3.0 Ghz) or higher OR AMD A10 7850B (3.0 Ghz) processor or higher OR Equivalent 64 bit x86 processor	
4.	Memory	8 GB DDR3 RAM @ 1600 MHz. One DIMM Slot must be free for future upgrade	
5.	Motherboard	OEM Motherboard	
6.	Hard Disk Drive	Minimum 500 GB SATA III Hard Disk @7200 RPM or higher	
7.	Audio	Line/Mic In, Line-out/Speaker Out (3.5 mm)	
8.	Network port	10/100/1000 Mbps auto-sensing on-board integrated RJ-45 Ethernet Port	
9.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/	
10.	USB Ports	Minimum 4 USB ports (out of that 2 must be in front)	
11.	Display Port	1 Display Port (HDMI/VGA) port	
12.	Power supply	Maximum Rating 250 Watts, 80 plus certified power supply	
13.	Keyboard	104 keys Heavy Duty Mechanical Switch Keyboard (USB Interface) with 50 million keystrokes life per switch. Rupee Symbol to be engraved.	
14.	Mouse	Optical with USB interface (same make as desktop)	
15.	Monitor	Minimum 18.5" diagonal LED Monitor with 1366x768 or higher resolution. (Same make as desktop). Must be TCO05 certified	
16.	Operation System and Support	Pre-loaded Windows 8.1 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. Can be downgraded to Windows 7 Professional (64 bit). All Utilities and driver software, bundled in CD/DVD/Pen-drive media	

Sr No	Item	Minimum Specifications	Bidder's offer
17.	Certification for Desktop	Energy Star 5.0 or above / BEE star certified	
18.	Other pre-loaded software (open source/ free)	Latest version of Libre-office, Latest version of Adobe Acrobat Reader, Scanning Software (as per scanner offered). These software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.	

7. Laptop

Sr No	Item	Minimum Specifications	Bidder's offer
1.	Make	Must be specified	
2.	Model	Must be specified	
3.	Processor	Our suggestion : Intel Core i3 with latest generation (1.9 Ghz) or higher OR AMD A10 PRO 7300 (1.9Ghz) Processor or higher OR Equivalent 64 bit x86 processor	
4.	Display	Minimum 14" Diagonal TFT Widescreen with minimum 1366 x 768 resolution (16:9 ratio)	
5.	Memory	4 GB DDR3 RAM @ must be free for future upgrade	
6.	Hard Disk Drive	Minimum 500 GB SATA HDD @ 5400 rpm	
7.	Ports	3 USB Ports 1- Gigabit LAN (RJ 45); 1- HDMI/Display port, 1- VGA, 1- headphone/Microphone;	
8.	Web Camera	Built in web cam	
9.	Wireless Connectivity	Wireless LAN - 802.11b/g/n/ Bluetooth 3.0	
10.	Audio	Built-in Speakers	
11.	Battery backup	Minimum 4 lithium ion or lithium polymer battery with a backup of minimum 4 hours	
12.	Keyboard and Mouse	84 Keys Windows Compatible keyboard, Integrated Touch Pad.	
13.	Operating System	Pre-loaded Windows 8.1 (or latest) Professional 64 bit, licensed copy with certificate of authenticity (or equivalent authenticity information) and all necessary and latest patches and updates. Can be downgraded to Windows 7 Professional (64 bit). All Utilities and driver software, bundled in CD/DVD/Pen-drive media	
14.	Certification	Energy Star 5.0 or above / BEE star certified	

Sr No	Item	Minimum Specifications	Bidder's offer
15.	Weight	Laptop with battery (without DVD) should not weigh more than 2 Kg	
16.	Accessories	Laptop carrying Back-pack. It must be from same OEM as laptop	
17.	Other pre-loaded software (open source/ free)	Latest version of Libre-office, Latest version of Adobe Acrobat Reader Scanning Software (as per scanner offered). These software shall be pre-loaded (at the facility of OEM or any other location) before shipment to Authority offices/locations.	

8. Network Colour Laser Printer

#	Parameter	Minimum Specifications
1.	Print Speed	Black : 16 ppm or above on A3, 24 ppm or above on A4 Colour : 8 ppm or above on A3, 12 ppm or above on A4
2.	Resolution	600 X 600 DPI
3.	Memory	8 MB or more
4.	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes
5.	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray
6.	Duty Cycle	25,000 sheets or better per month
7.	OS Support	Linux, Windows 2000, Vista, 7, 8, 8.1
8.	Interface	Ethernet Interface

10. Online UPS

#	Parameter	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at respective location
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
5.	Input Voltage Range	305-475VAC at Full Load
6.	Input Frequency	50Hz +/- 3 Hz
7.	Output Voltage	400V AC, Three Phase for over 5 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.	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
12.	Battery Backup	60 minutes in full load
13.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery
14.	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.
15.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.
16.	Cabinet	Rack / Tower type
17.	Operating Temp	0 to 40 degrees centigrade

11. Fixed Dome Camera for Indoor Surveillance

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
6.	Lens#	Auto IRIS 2.8-10mm
7.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264 individually configurable
8.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)
9.	IR Cut Filter	Automatically Removable IR-cut filter
10.	Day/Night Mode	Colour, Mono, Auto
11.	S/N Ratio	≥ 50 dB
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
13.	Wide Dynamic Range	True WDR upto 80 db
14.	Audio	Full duplex, line in and line out, G.711, G.726
15.	Local storage	microSDXC up to 32GB (Class 10) In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is required to transfer the SD card based recordings to server.
16.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S &G
17.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
18.	Intelligent Video	Motion Detection & Tampering alert
19.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface
20.	Operating conditions	0 to 50°C
21.	Casing	NEMA 4X / IP-66 rated & IK 09
22.	Certification	UL2802 / EN, CE ,FCC

#	Parameter	Minimum Specifications or better
23.	Power	802.3af PoE (Class 0) and 12VDC/24AC

12. Radio Handset

Bidder will have to visit Visakhapatnam Police Dept. and the Radio Handset should be similar to the one used by the Visakhapatnam Police Dept.

13. LCD Projector

#	Item	Minimum Specifications
1.	Display Technology	Poly-silicon TFT LCD
2.	Resolution	HD 1080p
3.	Colours	16.7 million Colours
4.	Brightness	2500 or more ANSI lumens (in Normal Mode)
5.	Contrast Ratio	2000:1 or more
6.	Video Input	One computer (D-Sub, Standard 15 pin VGA connector) One S-Video One HDMI
7.	Audio	Internal speaker
8.	Output ports	External Computer Monitor port, audio ports
9.	Remote Operations	Full function Infrared Remote Control
10.	Other features	Auto source detect, Auto-synchronisation, Keystone Correction

6.2. Smart Data Center and Disaster Recovery Infrastructure Components

a) Data Center and DR Locations

- Authority shall provide the location to house the compute and storage infrastructure, at the Data Center facility being built at the Smart City Operation Center building.
- The DR for the data shall be at the Cloud Data Center provider who is providing colocation, managed hosting and cloud services to Authority. The rate card, for various services offered by the vendor will also be available on request.
- Various ICT equipment to be provisioned and maintained by the SI at the Data Center & DR Sites are given below.

Technical Specifications for Smart Data Center and Disaster Recovery Infrastructure Components

b) WAN / Internet 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.	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 • 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

#	Item	Minimum Specifications
10.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate

c) Data Center TOR (Top of the Rack) Switch

#	Parameter	Minimum Specifications
1.	Ports	• 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra 2 numbers of Uplink ports (40GE) • All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports.
2.	Switch type	Layer 3
3.	MAC	Support 32K MAC address.
4.	Backplane	Capable of providing wire-speed switching
5.	Throughput	500 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	• IPV4, IPV6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support • Support up to 1024 VLANs • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection, • Should support Ring protection
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 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 a console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface
13.	Resiliency	• Dual load sharing AC and DC power supplies • Redundant variable-speed fans

d) 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	Minimum 64 GB Memory per physical server
3.	Internal Storage	2 x 300 GB SAS (10k rpm) hot swap disk with extensible bays
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.

e) Blade Chassis Specifications

The blade chassis shall have the following minimum technical specifications:

#	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 Red Hat Linux Oss 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.

f) Primary Storage

#	Parameter	Minimum Specifications
1.	Solution/ Type	• IP Based/iSCSI/FC/NFS/CIFS
2.	Storage	• Storage Capacity should be minimum XX TB (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
3.	Hardware Platform	• Rack mounted form-factor • Modular design to support controllers and disk drives expansion

#	Parameter	Minimum Specifications
4.	Controllers	• At least 2 Controllers in active/active mode • The controllers / Storage nodes should be upgradable seamlessly, without any disruptions / downtime to production workflow for performance, capacity enhancement and software / firmware upgrades.
5.	RAID support	• RAID 0, 1, 1+0, 5+0 and 6
6.	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.
7.	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
8.	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 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
9.	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

g) Secondary Storage

#	Parameter	Minimum Specifications
1.	Solution/Type	• Secondary Storage (Archival/Backup) can be on any media such as Tapes, Disks, Disk systems, etc. or its combination. (so as to arrive at lower cost per TB) • **May or may not use de-duplication technology** • Compatible with primary storage • Must use latest stable technology platform, with support available for next 7 to 10 years.
2.	Backup Size	To store data as required, to meet the archival requirement for different type of data/information
3.	Hardware Platform	• Rack mounted, • Rack based Expansion shelves
4.	Software Platform	Must include backup/archive application portfolio required
5.	Retrieval time	• Retrieval time for any data stored on secondary storage should be max. 4 hours for critical data & 8 hours for other data. This would be taken into account for SLA calculation. (Critical data means any data needing urgent attention by the Judicial System or by Police Dept. for investigation / terrorist treat perception).

h) Server/Networking Rack Specifications

#	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
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" dia (4 Nos. per Rack) • Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based - The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor
6.	Metal	Aluminium extruded profile
7.	Side Panel	Detachable side panels (set of 2 per Rack)

6.2.1.Core Router

#	Item	Minimum Specifications
1.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces

#	Item	Minimum Specifications
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, X.25, 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
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

6.2.2. Internet 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.	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 • 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

6.2.3. Firewall

#	Item	Minimum Specifications
1.	Physical attributes	• Should be mountable on 19” Rack • Modular Chassis • Internal redundant power supply
2.	Interfaces	• 4 x GE, upgradable to 8 GE • Console Port 1 number

#	Item	Minimum Specifications
3.	Performance and Availability	• Encrypted throughput: minimum 800 Mbps • 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
6.	Other support	• 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS
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

6.2.4. 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

#	Item	Minimum Specifications
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
8.	Management	• SNMP V1, 2C, 3 • HTTP, HTTPS • SSH, 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 usage per policy • IPS should have provision for external bypass Switch

6.2.5. Data Center Switch (1G)

(To be used for Data centre LAN 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

#	Parameter	Minimum Specifications
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 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

Data Center Switch (10 G)

(To be used as Top of the Rack (TOR) switch if required)

#	Parameter	Minimum Specifications
	Ports	• 24 or 48 (as per density required) 1G/ 10G Ethernet ports (as per internal connection requirements) and extra 2 numbers of Uplink ports (40GE) • All ports can auto-negotiate between all allowable speeds, half-duplex or full duplex and flow control for half-duplex ports.
1.	Switch type	Layer 3
2.	MAC	Support 32K MAC address.
3.	Backplane	Capable of providing wire-speed switching
4.	Throughput	500 Mpps or better
5.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks
6.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.
7.	Protocols	• IPV4, IPV6 • Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1X Security standards • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • DHCP support • Support up to 1024 VLANs • Support IGMP Snooping and IGMP Querying • Support Multicasting • Should support Loop protection and Loop detection, • Should support Ring protection
8.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication
9.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent
10.	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
11.	Management	• Switch needs to have a console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON • Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI, GUI based software utility and using web interface
12.	Resiliency	• Dual load sharing AC and DC power supplies • Redundant variable-speed fans

6.2.6.Server Load balancer

- Server Load Balancing Mechanism
  - Cyclic, Hash, Least numbers of users
  - Weighted Cyclic, Least Amount of Traffic
  - NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
- Redundancy Features
  - Supports Active-Active and Active-Standby Redundancy
  - Segmentation / Virtualization support along with resource allocation per segment, dedicated access control for each segment
- Routing Features
  - Routing protocols RIPv1/RIPv2/OSPF
  - Static Routing policy support
- Server Load Balancing Features
  - Server and Client process coexist
  - UDP Stateless
  - Service Failover
  - Backup/Overflow
  - Direct Server Return
  - Client NAT
  - Port Multiplexing-Virtual Ports to Real Ports Mapping
  - DNS Load Balancing
- Load Balancing Applications
  - Application/ Web Server, MMS, RTSP, Streaming Media
  - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
  - LDAP, RADIUS
- Content Intelligent SLB
- HTTP Header Super Farm
- URL-Based SLB
- Browser Type Farm
  - Support for Global Server Load Balancing
  - Global Server Load Balancing Algorithms
  - HTTP Redirection,
  - HTTP
  - DNS Redirection, RTSP Redirection
  - DNS Fallback Redirection, HTTP Layer 7 Redirection
- SLB should support below Management options
  - Secure Web Based Management
  - SSH
  - TELNET
  - SNMP v1, 2, 3 Based GUI
  - Command Line

6.2.7.Tape library

Sr 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

Sr No	Item	Minimum Specifications
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 Symatec Net Backup
11	Accessories	With all required cables and accessories to install and configure in standard 19" rack and to connect to Server/SAN switch

6.2.8. 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

6.2.9. 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

6.2.10. Back-up Software

1. The software shall be primarily used to back up the necessary and relevant video feeds from storage that are marked or flagged by the Police. The other data that would require backing up would include the various databases that shall be created for the surveillance system. Details of data that would be created are available in the table at section 'Data Requirements'
2. Scheduled unattended backup using policy-based management for all Server and OS platforms
3. The software should support on-line backup and restore of various applications and Databases

4. The backup software should be capable of having multiple back-up sessions simultaneously
5. 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
6. The backup software should support different types of user interface such as GUI, Web-based interface

6.2.11. Database Licenses

a) Bidder needs to provide Licensed RDBMS, enterprise/full version as required for the proposed Surveillance System and following all standard industry norms for performance, data security, authentication and database shall be exportable in to XML.

6.2.12. Enterprise Management System (EMS)

The Enterprise Management System (EMS) is an important requirement of this Project. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System

Proposed EMS Solution shall be based on industry standard best practice framework such as ITIL etc.

SLA & Contract management System

The SLA & Contract Management solution should enable the Authority to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the Surveillance project. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are -

- It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
- The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components
- The solution must follow governance, compliance and content validations to improve standardisation of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Surveillance Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system

- The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance

- The solution should support SLA Alerts escalation and approval process.

- Solution should support effective root cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.

- Accept Data from a variety of formats; provide pre-configured connectors and adapters, Ability to define Adapters to data source in a visual manner without coding.

- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project

- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.

- The solution should provide historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance

- Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF etc.

- The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardisation and governance of the surveillance project

- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project

- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)

    - Resource utilisation exceeding or below customer-defined limits

    - Resource utilisation exceeding or below predefined threshold limits

An indicative List of SLAs that need to be measured centrally by SLA contract management system are given in the Tender Document. These SLAs must be represented using appropriate customisable reports to ensure overall service delivery.

Network Management System

Solution should provide Fault, Configuration & Performance management of the entire datacentre infrastructure and should monitor IP\SNMP enabled devices such as Routers, Switches, Cameras, Online UPS, etc. Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation in order to measure central SLA's and calculate penalties. Following are key functionalities that are required, which will help measuring SLA's as well as assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

- 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 from central location to Zonal / Police Station Level.

- 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 as root cause of network problems and administrators should receive an alert in case of any change made on routers spread across surveillance project.

- Network Performance management system should provide predictive performance monitoring and should be able to auto-calculate resource utilisation baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits based on baseline data instead of setting up manual thresholds for monitored devices.

- The system must support the ability to create reports that allow the surveillance administrators to search all IP traffic over a specified historical period, for a variety of conditions for critical router interfaces.

- The proposed system must be capable of providing the following detailed analysis across surveillance domain:

    - Top utilised links (inbound and outbound) based on utilisation of link

    - Top protocols by volume based on utilisation of link

    - Top host by volume based on utilisation of link

- **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 the Surveillance 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.

    - The solution should provide a unified web based console, which consolidates all aspects of role based access under a single console.

    - Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.

Centralised Helpdesk System

- The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.

- Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.

- The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.

- Centralized Helpdesk System should have integration with Network/Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what particular alarms corresponding helpdesk tickets got logged.

- Surveillance Network admin should be able to manually create tickets through Fault Management GUI.

- System should also automatically create tickets based on alarm type

- System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.

6.2.13. Centralised Anti-virus Solution

a) Shall be able to scan through several types of compression formats.

b) Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)

c) Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)

d) Shall be able to scan only those file types which are potential virus carriers (based on true file type)

e) Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls

f) Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.

g) The solution must support multiple remote installations

h) Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.

i) Should be capable of providing multiple layers of defence

j) Shall have facility to clean, delete and quarantine the virus affected files.

k) Should support scanning for ZIP, RAR compressed files, and TAR archive files

l) Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.

m) Should use multiple scan engines during the scanning process

n) Should support in-memory scanning so as to minimize Disk IO.

o) Should support Multi-threaded scanning

p) Should support scanning of nested compressed files

q) Should support heuristic scanning to allow rule-based detection of unknown viruses

r) Updates to the scan engines should be automated and should not require manual intervention

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

t) Updates should be capable of being rolled back in case required

u) File filtering should be supported by the proposed solution; file filtering should be based on true file type.

v) Should support various types of reporting formats such as CSV, HTML and text files

w) Shall scan at least HTTP, FTP traffic (sending & receiving) in real time and protect against viruses, worms & Trojan horse attacks and other malicious code.

6.2.14. 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.

6.2.15. 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 (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.

- 12 mm thick fire line Gypsum false ceiling and lighting troughs 300 mm as per design including 100 mm high cornices as lighting pelmets on G.I. frame work, in G.I. vertical supports at every 450mm c/c and horizontal runners at every 900mm c/c self-taping metal screws to proper line and level. The same shall be inclusive of making holes and required framing for fixing electrical fixtures, A.C. grills etc. GI vertical supports to be anchored to slab by means of anchor fasteners.

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 fireline 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 cutouts 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 aluminum 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 fireline 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.

2. 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.

3. 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.

4. 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 need to be in place for this copper mesh.

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

5. 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 134standard 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.

6. Comfort Air Conditioning at Command Centers

- 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

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

Commissioning

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

ASPIRATING SMOKE DETECTION SYSTEM

- This specifications 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

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

Design Requirements

- 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 modeling 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, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.

Displays on the Detector Assembly

- 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

Sampling Pipe

- 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.

Installation

- 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.

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.

8. 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

6.2.16. Integration Capabilities

6) 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.

7) 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.

8) 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 Vizag Traffic police)
   - Access information of water management resources (Disaster management cell at Authority 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

9) 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

10) 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 optimized 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.

6.2.17. Other Requirements

6) 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 Authority network of services through an integration layer.

7) 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. SCADL takes the responsibility of necessary civil work including furniture through another tender process

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

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

10) **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 center at location decided by Authority to be provided by successful bidder. Further the platform will provide an open standards based integration Bus with API Management, providing full API lifecycle management with governance and security.

6.3. Red Light Violation Detection System

6.3.1. Functional Specifications

1) The following Traffic violations to be automatically detected by the system by using appropriate Non-Intrusive sensors technology:
   a) Red Light Violation
   b) Stop Line Violation
2) The system should be capable of capturing multiple infracting vehicles simultaneously in Different lanes on each arm at any point of time with relevant infraction data like:
   a) Type of Violation
   b) Date, time, Site Name and Location of the Infraction
   c) Registration Number of the vehicle through ANPR Camera system for each vehicle identified for infraction.
3) The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show nature of violation and proof thereof :-
   a) When it violates the stop line.
   b) When it violates the red signal.
   c) Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation.
4) The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be clearly identifiable and demarcated in the image produced by the camera system.
5) The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles with respect to the stop line and clearly indicate colour of the Traffic light at the instant of Infraction even if any other means is being used to report the colour of the light.
6) The system should interface with the traffic controller to validate the colour of the traffic signal reported at the time of Infraction so as to give correct inputs of the signal cycle.
7) The Evidence and ANPR camera should continuously record all footage in its field of view to be stored at the local base station. This should be extractable onto a portable device as and when required. The option of live viewing of evidence cameras from the locations shall be available at the CCC. The network should have the capability to provide the real time feed of the evidence camera to the CCC at the best resolution possible on the available network.
8) The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night time.

6.3.2. Recording & display information archive medium

The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:

1) Computer generated unique ID of each violation
2) Date (DD/MM/YYYY)
3) Time (HH:MM:SS)
4) Equipment ID
5) Location ID
6) Carriageway or direction of violating vehicle
7) Type of Violation (Signal/Stop Line)
8) Lane Number of violating vehicle
9) Time into Red/Green/Amber
10) Registration Number of violating vehicle

6.3.3. On site-out station processing unit communication & Electrical Interface

#	Parameter
1	The system should automatically reset in the event of a program hang up and restart on a button press. However the system should start automatically after power failure.
2	The system should have secure access mechanism for validation of authorized personnel.
3	Deletion or addition and transfer of data should only be permitted to authorized users.
4	A log of all user activities should be maintained in the system.
5	Roles and Rights of users should be defined in the system as per the requirements of the client
6	All formats of the stored data with respect to the infractions should be Non Proprietary.
7	The communication between the on-site outstation processing unit housed in the junction box and the detection systems mounted on the cantilever shall be through appropriate secured technology.
8	The system should have the capability to transfer the data to TCC through proper encryption in real time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer.
9	In the event that the connectivity to the TCC is not established due to network/connectivity failures, then all data pertaining to the infraction shall be stored on site and will be transferred once the connectivity is re-established automatically. There shall also be a facility of physical transfer of data on portable device whenever required. There should be a provision to store minimum one week of data at each site on a 24x7 basis.

6.3.4. Mounting structure

#	Parameter

1	Should be cantilever mounted and shall have minimum 6 Mtrs. height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.
2	It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.
3	It shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g Poles, Navigation boards etc) currently installed at these locations. The equipment should look "one" with the surroundings of the location and not look out of place.
4	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.

6.3.5. RLVD Application

#	Parameter
1	It should be capable of importing violation data for storage in database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The programme should allow for viewing, sorting, transfer & printing of violation data.
2	It should print the photograph of violations captured by the outstation system which would include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle along with all data as per clause 4.
3	All outstation units should be configurable using the software at the Central Location.
4	Violation retrieval could be sorted by date, time, location and vehicle registration number and the data structure should be compatible with Police database structure. It should also be possible to carry out recursive search and wild card search.
5	The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with traffic signal, connectivity failure, Camera tampering, sensor tampering).
6	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 75% or better during the day time and 40% or better during the night time with a standard number plate.
7	The application software should be integrated with the E Challan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period by the SI.
8	Image zoom function for number plate and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases the printing should be possible along with the magnified image.
9	Various users should be able to access the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.

10	Apart from role based access, the system should also be able to define access based on location.
11	Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
12	Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. Considering the high sensitivity of the system, design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
13	The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft etc. Provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.
14	The evidence of Infraction should be encrypted and protected so that any tampering can be detected.
15	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.
16	System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used.
17	The user interface should be user friendly and provide facility to user for viewing, sorting and printing violations. The software should also be capable of generating query based statistical reports on the violation data.
18	The data provided for authentication of violations should be in an easy to use format as per the requirements of user.
19	User should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).
20	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.
21	Log of user actions be maintained in read only mode. User should be provided with the password and ID to access the system along with user type (admin, user).
22	Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behavior is recorded including (Speed of violating vehicle, notified speed limit, Signal Jumping, Stop Line Violation, Speed Violation with Registration Number Plate Recognition facility.

23	Number plate should be readable automatically by the software/interface. There should be user interface for simultaneous manual authentication / correction and saving as well.
24	Interface for taking prints of the violations (including image and above details).

6.3.6. Technical Specifications

S. No.	Description	
1.	**General**	
	The system should be capable of generating a video in any of the standard industry formats (MJPEG, avi, mp4, mov, etc) with at least 10 frames per second. The video shall be from t-5 to t+5 sec of the violation and should also be recorded (t being the instant at which the infraction occurred).	
2.	**Digital Camera/Automatic Number Plate Recognition(ANPR) camera**	
a.	Sensor Type	Progressive scan CCD/CMOS Day/Night Camera
b.	Resolution	2 Megapixels or better
c.	Video Compression:	Motion JPEG,H.264
d.	Normal Horizontal Field of View	at least 3.5 Mtr. (One lane)
e.	Typical Range	30 Mtrs. or better
f.	Operating Temp.	-5 to +60 Degree C
g.	Auto Iris Control	Yes
h.	Protection rating	IP66 , IK10 rated or better standards capable of withstanding vandalism and harsh weather conditions.
3.	**On site-out station processing unit communication & Electrical Interface (Junction Box)**	
a.	Data Storage on site	The system should be equipped with appropriate storage capacity for 7 days 24X7 recording, with overwriting capability. The images should be stored in tamper proof format only.
b.	Network Connectivity	Wired/GPRS based wireless technology with 3G upgradable to 4G capability.
c.	Minimum 2(two) USB Port to support the latest external mass storage devices and Ethernet (10/100) Port for possible networking. However all logs of data transfer through the ports shall be maintained by the system.	
d.	The system should be capable of working in ambient temperature range of -5^{o}C to 60^{o}C.	

e.	Lightening arrester shall be installed for safety of system (As per BIS standard IS 2309 of 1989).
f.	The housing(s) should be capable of withstanding vandalism and harsh weather conditions and should meet IP66, IK10 standards (certified).
4.	**Violation Transmission and Security**
a.	Encrypted data, images and video pertaining to Violations at the Onsite processing station should be transmitted to the CCC electronically through GPRS based wireless technology with 3G upgradable to 4G, in Jpeg format.
b.	Advanced Encryption Standard (AES) shall be followed for data encryption on site and CCC, and its access will protected by a password.
c.	The vendor shall ensure that the data from the onsite processing unit shall be transferred to CCC within one day.
5.	**Video Recording**
a.	The system should be capable of continuous video recording in base station for 7 days. The system shall automatically overwrite the data after 7 days. It should be noted that at any point of time the local storage at the base station should have the data of previous 7 days.
b.	Direct extraction through any physical device like USB, Hard disk shall be possible

6.3.7. Face Recognition System

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

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

The system shall be able to:

i. Capture face images from CCTV feed and generate alerts if a blacklist match is found.
ii. Search photographs from the database matching suspect features.
iii. Match suspected criminal face from pre-recorded video feeds obtained from CCTVs deployed in various critical identified locations, or with the video feeds received from private or other public organization's video feeds.
iv. Add photographs obtained from newspapers, raids, sent by people, sketches etc. to the criminal's repository tagged for sex, age, scars, tattoos, etc. for future searches.
v. Investigate to check the identity of individuals upon receiving such requests from.
vi. Enable Handheld mobile with app to capture a face on the field and get the matching result from the backend server.

The facial recognition system shall be enabled at cameras identified by the Authority. These cameras identified shall be installed at critical locations finalized by authority

The facial recognition system in offline mode shall be provided by the SI in line with the requirement specified in the RFP.

The detailed functional requirement specification of the facial recognition system is provided in subsequent sections of this RFP.

1) Face Image Data Standard

Manual Facial recognition is not sufficient currently for de-duplication. . Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image is also recommended.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt **ISO /IEC 19794-5:2005(E)**. While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection.

The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

Standard	Description
ISO /IEC 19794-5:2005(E)	This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications. The scope of this standard includes: o Characteristics of Face Image capturing device o Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification o Scene requirements of the face images, keeping in view a future possibility of computer based face recognition o Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

6.4. Smart Environmental Sensors

6.4.1. Functional Specifications

a) Smart environment sensors will gather data about pollution, temperature, rains, levels of gases in the city (pollution) and any other events on a daily basis. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.

b) The environment sensors should be have the following capabilities:

- They should be rugged enough to be deployed in open air areas, on streets and parks
- They should be able to read and report at least the following parameters: Temperature, Humidity, Ambient Light, Sound, CO, NO2, NOX, CO2, SO2.

c) Smart environment sensors will enable citizen to keep a check on their endeavors which impact environment and enable the city to take remedial action if required. These environmental sensors can also be connected via 3G or 4G wireless network. It is not mandatory to connect all sensors via MPLS fiber network.

d) The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.

e) Successful bidder can also make use of the nearby variable messaging displays wherever possible.

f) The sensor management platform should allow the configuration of the sensor to the network and also the locational details etc.

g) Bidder needs to make relevant information available on the displays along with other environmental sensor data in consultation with Authority. If data is available in any existing external system of Authority, then the same shall be integrated by the bidder with the Command & Control System.

h) Additionally, the bidder should install water level monitoring (flood sensors) at low lying areas of the city. These locations may differ from the locations of other environmental sensors and need to be finalized after the detailed survey of locations by the successful bidder, in consultation with Authority. The bidder should consider implementation of these sensors across the specified locations.

i) The environment sensors will measure and log the data from locations described in the subsequent sections of the bid document.

6.4.2. Technical Specifications

#	Parameter	Specification
1.	Measurement principle	• Temperature, Humidity, Ambient Light, Sound, CO, NO2, NOX, CO2, SO2
2.	Measurement component Measurement range	• NO2: 0 to 10 ppm • NOX : 0 to 50ppm , 5000ppm • SO2 : 0 to 500 ppm • CO : 0 to 50ppm, 5000ppm • O3: up to 1000 ppb • CO2 : 0 to 10% / 0 to 20% • 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)
3.	Rain Water measurement	• Rainfall in millimetres (mm)
4.	Water levels (for flood monitoring)	• Data integration with existing system (APIs will be provided)
5.	Repeatability	• ±0.5% FS
6.	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
7.	Temperature and Humidity Sensor	• Real-time Temperature Range: Indoor -10ºC ~ +70ºC (+14ºF ~ +122ºF) • Real-time in Air Humidity Level Display (up to 100%)
8.	Span drift	• ±2.0% FS max./week • ±2.0% FS max./month for O2 meter
9.	Response speed	• 120 seconds max. for 90% response from the analyzer inlet
10.	Connectivity (Minimum)	• USB / Ethernet connectively to graphical display

6.5. Variable Messaging Display Board (VMD)

6.5.1. Functional Specifications

a) VMD will be installed at identified strategic locations. The location of VMDs will be on the key junctions (mostly on the sides without obstructing the traffic) and other strategic locations with large foot fall. The VMD software application will allow user to publish specific messages for managing traffic and also general informative messages.

b) VMD will enable Authority to communicate effectively with citizens and also improve response while dealing with exigency situations. These will also be used to regulate the traffic situations across the city by communicating right messages at the right time.

c) The variable message display shall consist of variable message signboard with local controller, for local controls in few situations.

d) A VMD software system shall be provided to the Command and Communications Center for message preparation monitoring and control of the variable message signs. IP based Network equipment shall be provided to connect the VMD with the VMD software system.

e) VMD software application will provide the normal operator to publish predefined sets of messages (textual / image). 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.

f) VMD software application will allow an operator to seamlessly toggle between multiple VMS points at each workstation in order to send specific messages to specific locations, as well as sending common message to all VMDs.

g) VMD software application will accommodate different access rights to various control unit functionalities depending on operator status and as agreed with the client. Software should be GUI based, and capable to handle 200 VMS signage. User should be able to select desired location in Map and this should enable user to see the live status of that specific VMD.

h) The variable messaging displays can also be used for advertisement purposes. Approximately 20% of the total running time will be utilized by Authority for its own discretion whereas the remaining time can be used by the SI for advertisement purpose.

i) The land for VMDs will be provided to the SI at no extra cost. Also no rental/lease charges will be levied on the bidder for using the land for Variable Message Signboards.

6.5.2. Technical Specifications

i. Display

#	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.	Colour	True Colour
3.	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
4.	Luminance Class	L-3 as per EN 12966
5.	Contrast Ratio	R2-R3 as per EN 12966
6.	Beam Width	B6+ : Viewing angle shall ensure message readability for citizens, motorists, pedestrians, etc. on the respective locations
7.	Display capability	• Fully programmable, full colour, full matrix, LED displays • Alpha-numeric, Pictorials, Graphical & video
8.	Display Language	• To support both pictograms and bilingual (English and Devanagari) text
9.	Display Front Panel	• It shall utilize a front face that is smooth, flat, scratch-resistant, wipe-clean • 100% anti-glare
10.	Message Creation	Through both a Central Control Room Application and a local Laptop/Device loaded with relevant software
11.	Language	Multilingual (Marathi/English/Hindi) and all fonts supported by windows
12.	Auto Dimming	Auto dimming adjusts to ambient light level.
13.	In built Sensor	Photoelectric sensor
14.	Storage capacity	Minimum 60 GB
15.	Display Area	Display size of VMD should be 2.88 x 1.92 meters
16.	Number of Lines & Characters	The number of lines and characters can be customized as per the requirement (Min 3 Lines & 10 Characters)
17.	Brightness & contrast	Controlled through software
18.	Display Driving method	Direct current control driving circuit. Driver card of display applies Direct Current Technology
19.	Display Style	Steady, flash, partial flash, right entry, left entry, top entry, bottom entry, canter spread, blank, and dimming
20.	Connectivity	IP Based
21.	Access Control	Access control mechanism would be also required to establish so that the usage is regulated.

#	Specifications	Minimum Requirements
22.	Integration	• Interface with GPRS or Ethernet • Integration with Command and Communications Center and service providers for offering G2C and B2C services
23.	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.
24.	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
25.	Power	Automatic on/off operation
26.	Casing	• Weather-proof Display for VMS • IP-66 rated for housing all control equipment
27.	Operating conditions	0° to 55°C
28.	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.

ii. Application Software for VMS (Control Messaging Application at Data Center)

The Application System for Controlling Messaging for VMS shall:

1) Be deployable over multiple (3 to 4) workstations.
2) Ensure that provision for feeding/updating the following information:
    a. VMS messages and information
    b. Types of possible scenarios per VMS
    c. Types of possible messages to be displayed on each VMS 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 VMS 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.

6.6. Public Address System

6.6.1. Functional Specifications

a) The Public Address System (PA) should be capable of addressing citizens at specific locations from the Command and Communications Center.

b) The proposed system shall contain an IP-based announcing control connected to the Command and Communications Center.

c) Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Authority to make important announcements for the public. It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations. The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.

d) The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).

e) The SI shall describe in detail the design, operational and physical requirements of the proposed public announcement system to demonstrate compliance with all the specified requirements of RFP.

f) PA system's master controller should have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.

g) PA system's master controller should facilitate multiple MIC inputs and audio inputs.

6.6.2. Technical Specifications

#	Parameter	Minimum Specifications or better
1.	PAS system	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs
2.	Speakers	• Minimum 2 Speaker, to be used in different directions • Minimum 200 Watts of amplification
3.	Connectivity	IP Based
4.	Access Control	Access control mechanism would be also required to establish so that the usage (including sound volume) is regulated.
5.	Integration	Command and Communications Center, Police Command Control Center, Traffic Control Center
6.	Battery	Internal Battery with different charging options (Solar/Mains)
7.	Power	Automatic on/off operation
8.	Casing	IP-65 rated for housing

#	Parameter	Minimum Specifications or better
9.	Operating conditions	0° to 50°C

6.7. Emergency Call Box

6.7.1. Functional Specifications

a) The emergency box (or panic button) will enable citizens to establish a two way audio (microphone and speaker) & camera (video camera and a video screen) communication link with Police (or / and with Authority's Disaster Management Cell or Command and Communications Center) through a press of a button.

b) Emergency/ Panic buttons to be strategically located, suitably sized and identified/clearly labelled for "Emergency".

c) The emergency feature must also be available within the mobile app which will enable the user to initiate a bidirectional audio call with Police /Command and Communications Center.

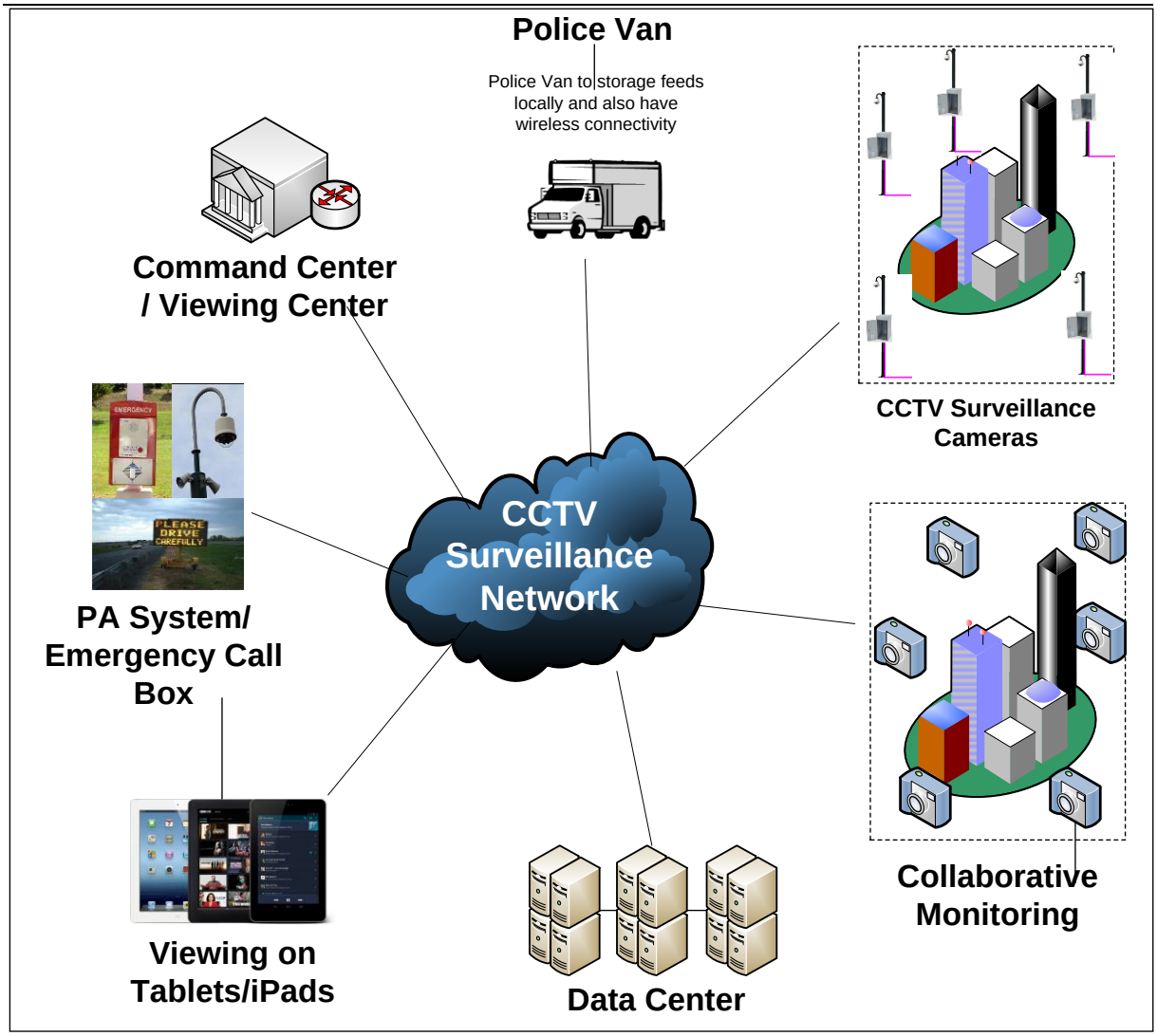
d) The unit shall preferably have a single button which when pressed, shall connect to Authority.

6.7.2. Technical Specifications

#	Parameter	Minimum Specifications or better
1.	Construction	Cast Iron/Steel Foundation, Sturdy Body for equipment
2.	Call Button	Watertight Push Button, Visual Feedback for button press
3.	Speaker & Microphone	VOIP Phone, Hands-free calling, Watertight and industrial grade equipment
4.	Connectivity	3G/4G/Ethernet/Fibre as per solution offered
5.	CCTV Camera	IP based, Color camera with minimum D1 resolution, Day/Night mode operations
6.	Battery	Internal Battery with different charging options (Solar/Mains)
7.	Power	Automatic on/off operation
8.	Casing	IP-65 rated for housing
9.	Operating Conditions	0° to 50°C
10.	Certification	UL/CE/EN

6.8. City Surveillance

A High level system overview of the proposed CCTV Surveillance System for Vizag City is given in the diagram below:



Feed/Message to Police Van is optional

6.8.1. Surveillance Equipment

The project includes surveillance of about across Vizag City. These locations would get covered through different types of surveillance cameras including Fixed Box Camera and PTZ Cameras.

The Implementation vendor (SI) shall asses the feasibility to use any existing electricity, phone or advertisement poles during initial site surveys. SI shall also asses the feasibility of leveraging other structures such as areas under a bridge or billboards. For the locations identified for re-purposing the existing poles or structures, an agreement shall be signed between the SI, Authority, and other relevant stakeholders for use of the facility for the Vizag City CCTV Surveillance Project.

UPS requirement (with minimum 30 minutes backup) is mandatory at 25% cameras. SI should ensure that proper protection is taken against power surges and ensure power stabilization to the surveillance equipment. The System Integrator would need to follow required earthing standards (e.g. IS-3043) and ensure that pole and the edge level components are protected against lightning. In addition, Junction box design should be modular and each component should be well organized and clamped inside to ensure components do not heat up or fall out on opening. For Electricity / Power, SI to bear the initial provisioning charge while recurring charge to be reimbursed by Vizag Municipal Corporation on actuals.

Select locations would be identified for ANPR cameras. If ANPR recognition fails, these cameras should at least be able to capture a clear image of license plate for investigation purposes.

The proposed video surveillance system will involve setting up of IP based outdoor security cameras across various locations in the Vizag City. The video surveillance data from various cameras deployed will be stored and monitored at Command control centers and Viewing center at Office of Commissioner of Police, Vizag

Other Smart Safety Components

Along with the components of the CCTV Surveillance system, the SI would be responsible to integrate the following services with the CCTV Surveillance system to build an infrastructure for a Smart city system in the Vizag Area.

Information security policy, including policies on backup
System Integrator shall be asked to prepare the Information Security Policy for the overall project, which would be reviewed & finalized by the Vizag City Authority & its Consultant. It is proposed that Security policy would be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests. The Systems Integrator shall obtain ISO 27001 certification for the CP Office Control Center within 2 quarters of final acceptance test. Payment from 3rd Quarter to be withheld till this certification is obtained by the successful bidder.

6.8.2. Functional Requirement of the City Surveillance System

Functional Requirement of the overall Surveillance System can be categorized into following components:

- Information to be Captured by Edge Devises
- Information to be Managed at the Command Center
- Command Center Requirements
- Information to be made available to different Police Personnel
- Operational Requirements
- Storage / Recording Requirements
- Other General Requirements

Information to be captured by Edge Devises

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized data center and would capture the video feeds at 15 FPS for majority of the time and at 8 FPS for the lean period. However, Authority may take the regular review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 0.5% of the cameras would be required to be viewed at higher FPS at a given point of time).

The complete tracking of a 'wanted' vehicle identified or flagged by Police should be possible on the GIS map.

It is recommended to clearly identify in SLAs that cameras need to transmit quality video feed (appropriately focused, clear, un blurred, jitter free, properly lit, unobstructed, etc.). Packet loss to be less than 0.5%.

Information to be analyzed at the Command Centers

The proposed Video Management System shall provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control center and the IP Network would create a virtual matrix, which would allow switching of video streams around the system.

Not all the cameras would be simultaneously viewed at Command & Communications Centers. Command Center shall from time to time take decisions on utilization of Alerts / Exceptions / Triggers generated by cameras, and specify the client machines where these would get populated automatically.

Police personnel shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of police officer)
- Accessibility to advanced analytics on recorded footages
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

Command Center Requirements

- Alarm Monitor

  Alarm Monitors must show the name of alarms when generated. The layout must not be restrictive.

- Guard Tours

  System should allow automatic launching of Guard Tours based upon factors like Time / Date / Bookmarked event

- Customizable and programmable Event Response Mechanism

  All the Event Response Mechanisms must be customizable based upon functional parameters like criticality, region, access, automatic/manual etc. (not limited to these four). SOPs for the daily

incident management to be designed and approved by Police Personnel and same must be implementable in the system.

System must allow generation of reports for all Incidents based upon filters like Criticality, Current Status, Date / Time (not limited to these). System to support excel/pdf for export.

- Quick and easy integration to 3rd Party systems

  System must support API based integration with other systems like eChallan, CCTNS etc. or any other 3rd Party system with allows API based integration

Other functionalities like Proper Device Grouping and User Management (including PTZ privileges) must be exportable at the access level of the user of the system for the review by the concerned authorities. Export file can be an Excel file or pdf. User must be able to export access report at his/her own level of authority.

Dashboards generated by the system (functional / technical) must be customizable based upon the user's requirements. The system must remember the edits done by the user to his/her own dashboard when he logins next time in the system.

System should allow generation of Audit Reports for the perusal of concerned Police Authorities.

Role Based Access to the Entire System

Various users should have access to the system using single sign on and should be role based. Different roles which could be defined (to be finalized at the stage if SRS) could be Administrator, Supervisor, Officer, Operator, etc. Apart from role based access, the system should also be able to define access based on location. Other minimum features required in the Role Based authentication Systems are as follows:

- The Management Module should be able to capture basic details (including mobile number & email id) of the Police Personnel & other personnel requiring Viewing / Administration rights to the system. There should be interface to change these details, after proper authentication.
- Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
- Biometric standardized coupled with login name & password should be enabled to ensure that only the concerned personnel are able to login into the system.
- Surveillance System should have capability to map the cameras to the Police Personnel from different. There should be interface to change these mappings too.
- For PTZ cameras, there should be provision to specify hierarchy of operators / officers for control of the cameras from various locations.

Storage / Recording Requirements

It is proposed that the storage solution is modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. As decided in the meeting of consultants & Vizag City Police Officials following storage requirements are proposed for the project:

- **The storage solution proposed is that the video feeds would be available for 30 days**. After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident in question would be stored until the Police deem it good for deletion.

- For incidents that are flagged by the Police or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted.
- Regardless of the above, the image of the License plate extracted by ANPR software, along with the timestamp and location of the image capture will stored for a period of 3 months
- Full audit trail of reports to be maintained for 90 days.
- Retrieval time for any data stored should be max. 4 hours for critical data & 8 hours for other data.
- The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.
- The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
- The system shall support H.264 or better, MPEG-4 and MJPEG compression formats for all analog cameras connected to encoders and all IP cameras connected to the system.
- The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server.
- The system should not limit amount of storage to be allocated for each connected device.
- The on-line archiving capability shall be transparent and allow Clients to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
- The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
- The system shall support Archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.
- Bandwidth optimization
    - The Recording Server / System shall offer different codec (H.264, MJPEG, MPEG-4, etc.) and frame rate (CIF, 4CIF, QCIF) options for managing the bandwidth utilization for live viewing on the Client systems.
    - From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
- The Recording Server / System shall support Camera (analogue and IP cameras) devices from various manufacturers.
- The Recording Server / System shall support the PTZ protocols of the supported devices listed by the camera OEMs.
- The system shall support full two-way audio between Client systems and remote devices.
- Failover Support

- The system shall support automatic failover for Recording Servers. This functionality shall be accomplished by Failover Server as a standby unit that shall take over in the event that one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online.
- The system shall support multiple Failover Servers for a group of Recording Servers.

- SNMP Support
  - The system shall support Simple Network Management Protocol (SNMP) in order for third-party software systems to monitor and configure the system.
  - The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.

Other General Requirements

Management / Integration functionality

- The Surveillance System shall offer centralized management of all devices, servers and users.
- The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
- The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
- It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
- The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
- System should be able to be integrated with Event Management / Incident Management System, if implemented by Vizag City Authority/ Vizag Municipal Corporation in future.

System Administration functionality

- The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
- The System Administration Server shall support different logs related to the Management Server.
  - The System Log
  - The Audit Log
  - The Alert Log
  - The Event Log
- Rules

  The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:

- Start and stop recording
- Set non-default live frame rate
- Set non-default recording rate
- Start and stop PTZ patrolling
- Send notifications via email
- Pop-up video on designated Client Monitor recipients

Client system

The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

Remote Web Client

The web-based remote client shall offer live view of up to 16 cameras, including PTZ control and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.

a) User Authentication – The Remote Client shall support logon using the user name and password credentials.

Matrix Monitor

a) Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.

b) The Matrix Monitor feature shall access the H.264/MJPEG/MPEG4 stream from the connected camera directly and not sourced through the recording server.

Alarm Management Module

a) The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.

b) The alarm management module shall provide interface and navigational tools through the client including;

i. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.

ii. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.

c) The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.

d) Basic VMS should be capable to accept third party generated events / triggers

Other Miscellaneous Requirements

- System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and SI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose. SI will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.
- All the systems proposed and operationalisation of Video Management System should comply with requirements of IT Acts.
- Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. Vizag City Authority may provide such tablets / smart phones to the designated Police Personnel. It will be responsibility of SI to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users so that uploading of video / pictures to the surveillance system is possible

There would be the provision for Third party audit periodically, paid by Authority separately

Video Management System

Video management system shall constitute of a platform which will be designed for viewing, recording and replaying acquired video as part of overall project solution. This platform will be based on the Internet Protocol (IP) open platform concept. Major functionalities are described here:

VMS Overview

1. VMS shall be used for centralized management of all field camera devices, video servers and client users.
2. VMS server shall be deployed in a clustered server environment/Support in built for high availability and failover for directory & recording servers
3. VMS shall support a flexible rule-based system driven by schedules and events.
4. VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
5. VMS shall support internet protocol (IP) cameras from major vendors.
6. The Contractor shall clearly list in their proposal the make and models that can be integrated with the VMS, additionally all the offered VMS and cameras must have Open Network Video Interface Forum (ONVIF) compliance.
7. VMS shall be enabled for any standard storage technologies and video wall system integration.
8. VMS shall be enabled for integration with any external Video Analytics Systems both edge & Server based

9. VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.
10. 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.
11. VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
12. VMS day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
13. Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and also for pre- and post-alarm recording display.
14. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
15. All CCTV camera video signal inputs to the system shall be provided to various command control center(s), viewing center etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
16. VMS client shall have the capability to work with touch enabled multi-monitor workstations. It shall be capable of displaying videos in up to three (3) monitors simultaneously.
17. VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
    a) AVI files
    b) MP4 Export or latest
18. For 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
19. All streams to the above locations shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.
20. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device:
    a) Brightness
    b) Contrast
    c) Color
    d) Sharpness
    e) Saturation
    f) Hue
    g) White balance
21. The VMS shall support the following operations:
    a) Adding an IP device
    b) Updating an IP device
    c) Updating basic device parameters
    d) Adding/removing channels
    e) Adding/removing output signals
    f) Updating an IP channel
    g) Removing an IP device
    h) Enabling/disabling an IP channel
    i) Refreshing an IP device (in case of firmware upgrade)

22. The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage.
23. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
24. The VMS shall allow the administrator to distribute camera load across multiple recorders and be able shift the cameras from one recorder to another by simple drag and drop facility.
25. VMS shall support automatic failover for recording .Some Critical cameras shall also be supported for Redundant (Mirrored Recording simultaneously)
26. VMS shall support manual failover for maintenance purpose.
27. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
28. VMS shall support integration with the ANPR application
29. VMS shall support integration with other online and offline video analytic applications.
30. VMS shall be able to accept alerts from video analytics built into the cameras, other third party systems, sensors etc.
31. VMS shall support manual failover of Directory for maintenance purpose
32. System should support recording management to view the recordings available on a camera's local storage device (such as an SD card), and copy them to the server.

Client system

The Client system shall provide remote users with rich functionality and features as described below.

1. Viewing live video from cameras on the surveillance system
2. Browsing recordings from storage systems
3. Creating and switching between multiple of views.
4. Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
5. Using digital zoom on live as well as recorded video.
6. Using sound notifications for attracting attention to detected motion or events.
7. Getting quick overview of sequences with detected motion.
8. Getting quick overviews of detected alerts or events.
9. Quickly searching selected areas of video recording for motion (also known as Smart Search).
10. The VMS shall use its own streaming server to efficiently steam the videos.
11. When the VMS client is set to view the live videos in say 3x3, 4x4 and 5x5 grids, the VMS should display lower resolution, high frame rate video to avoid high bandwidth and CPU usage on the VMS client
12. When the user selects a particular camera and wants to view it in full screen, the VMS should automatically show the highest quality and high frame rate video.

Web Client

1. The web-based remote client shall offer live view of up to 8 cameras, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.
2. User Authentication – The Remote Client shall support logon using the user name and password credentials

Mobile Client

The Contractor shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure

manner. It will be responsibility of contractor to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users. Communication between Mobile Client and Server shall be encrypted with Digital Certificates.

Alarm Monitoring

1. The VMS shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. It shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.
2. It shall provide interface and navigational tools through the client including;
3. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
4. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
5. It shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
6. Basic VMS should be capable to accept third party generated events / triggers

Other functionality

1. The Surveillance System shall offer centralized management of all devices, servers and users.
2. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
3. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
4. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
5. System should be able to be integrated with PSIM / Incident Management System.
6. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
7. The System Administration Server shall support different logs related to the Management Server.
    a) The System Log
    b) The Audit Log
    c) The Alert Log
    d) The Event Log
8. Rules: The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:
    a) Start and stop recording
    b) Set non-default live frame rate
    c) Send notifications via email
    d) Pop-up video on designated Client Monitor recipients

- Security Platform shall have strong security mechanism such as the use of advance encryption, digital certificates and claims-based authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.
- System should support Report and View Open Incident Cases. This also support associating the video footages pertaining to the incident either received from City CCTV

Cameras or shared by public to the police agency. This also allows viewing and downloading and delete Incident clips that are stored on the server by the administrator.

Failover & Redundancy

1. Synchronized Failover directory feature should be provided with the offered system to avoid the single point of failure. Also the system should sustain all its current operations i.e. recording, playback and live video even in the event of primary as well as failover directory failure. This functionality can either be loaded on any of the recording server or on a dedicated server. If offered software need dedicated server for this, then the same will be in contractor's scope. Specifications of failover administration server should be same as that of recording server except storage size.
2. Automated Failover recording should be provided to maintain the reliability of the system. In case of failure of one or more of primary recording servers simultaneously. Additional servers/storage required to meet this requirement should be in Contractors scope.
3. Redundant recording/Dual recording feature of the VMS should be supported by VMS. System administrator should get the privilege to configure this feature on any cameras simultaneously depend on the criticality of the cameras.
4. The VMS shall allow for 2-way audio communication using amplifier/call station connected the IP cameras in the field without any need of audio cabling from camera to control room

Video Analytics

General Requirements:

1. The Video Analytics shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for devices from different vendors.
2. Support any architecture namely distributed, centralized and hybrid
3. Support system openness without using any proprietary format
4. Support commercial-off-the-shelf computing hardware without the need of any proprietary hardware
5. Able to produce reliable analytics at lower resolutions like 4CIF resolution in order to save the computation
6. Able to process at variable resolution and frame rate when if necessary
7. It shall support open platform Video Management System (VMS).
8. It shall provide ONVIF device discovery
9. It shall get video from camera or VMS and send alarms to VMS to be viewed in VMS client
10. It shall stream the Analytics Video to VMS using open interface protocol like ONVIF.
11. It shall support multiple regions of analytics on single video feed.
12. It shall support multiple features to be enabled for each of the regions.
13. It shall support feature based scheduling so that that alarms can be enabled or disabled for a certain period of time.
14. 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.
15. It shall support both indoor and outdoor environment.
16. It shall support setting of minimum and maximum object size for detection.
17. It shall support masking of area in a view.

18. It shall support object masking.
19. It shall support color detection for vehicle & Object.
20. It shall support alarms to filter based on object color, size, speed and aspect ratio.
21. It shall support analytics capability to run both on server as well as edge (on camera).
22. It shall support simultaneous running of different features both on edge as well as server for same camera
23. It shall support camera independent licensing

Suspicious incident detection

1. It shall detect person loitering in a virtual area for more than a pre-defined period.
2. 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.
3. The VA shall support dense and sparse crowds for crowd counting and crowd flow detection
4. The VA shall detect object left out or abandoned in a virtual area by a person beyond a certain pre-defined period.
5. The VA shall detect object removed by a person beyond a certain pre-defined period.
6. The VA shall detect counter flow of people (such as people moving in a wrong way)

Traffic Management Features

1. It shall detect vehicle or group of vehicle moving in a wrong way.
2. It shall detect a vehicle parked in an area for a pre-defined period.
3. It shall detect congestion due to vehicles.

Other features

1. It shall be able to stitch up to 4 camera videos with overlapped view and provide the stitched view.
2. 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.

3. 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
1. It shall provide video summary of all the alarms.
2. It shall provide reporting option to export reports of alarms in PDF, EXCEL and Image formats and also option to schedule it.
3. It shall support email and FTP of alarm data and also option to schedule it.
4. It shall be able to provide comparison reports for different months and year

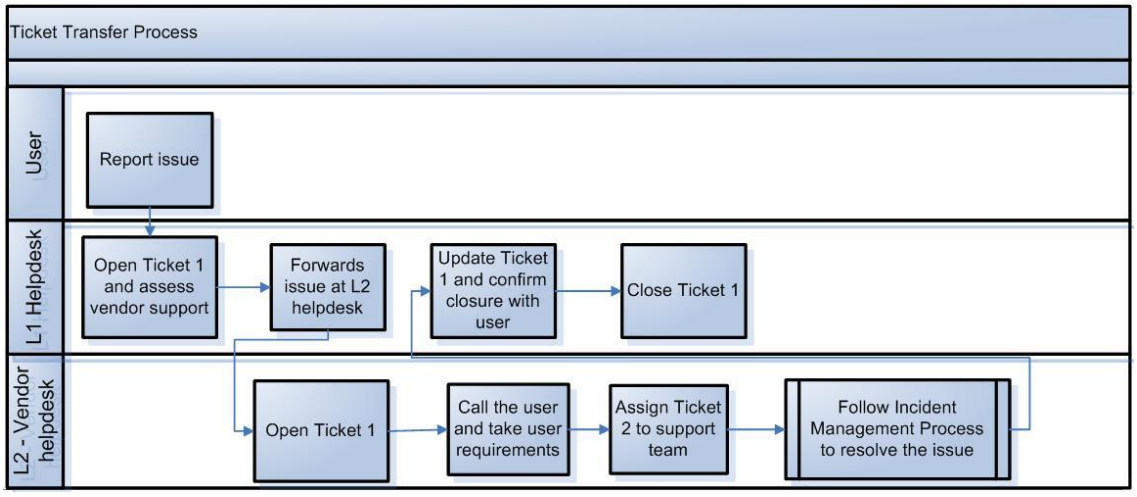
Helpdesk Management

It is envisaged that the centralized helpdesk, functioning as proposed below, would be managed by the Systems Integrator and shall serve following objectives:

- Act as the Point of Contact for the users of Surveillance System

- Own an Incident throughout its Lifecycle
- Communicate effectively with Police / Home Dept. Officers and IT support teams.
- Maintain high user satisfaction levels
- Maintain the SLA statistics & submit quarterly report to Police / Home Department

A general process flow for the helpdesk management is depicted in the flow-chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with the Vizag City Authority & its Consultant prior to the Go Live date.



System Integrator shall deploy a State-of-Art Enterprise Management System to handle the complexity of Operations & SLA Management defined in the DPR

Standardized Signs for CCTV Camera Locations

It is necessary that the CCTV Camera locations put some standardized signs informing the public of the existence of CCTV cameras. This will bring about the transparency on installation of CCTV cameras and no one would be able to later complaint for breach of privacy. Following tables give draft specifications for the signage to be put at the camera locations.

#	Item	Specifications
1	Size	Board Width = 8" / 12" (For type A and B) Board Width = 12" / 18" / 24" (For type C and D)
2	Plate Material	Corrosion resistant Aluminum Alloy as per IRC 67:2001 (Code of Practice for Road signs)
3	Plate Thickness	Minimum 1.5 mm
4	Retro-Reflective sheeting for sign-plate	Weather-resistant, having colour fastness

#	Item	Specifications
5	Other Specifications	As per IRC 67:2001 (Code of Practice for Road signs)
6	Mounting	Can be mounted on wall or pole (appropriate mounting brackets to be provided)
7	Design	As per following signage diagrams

6.8.3. Fixed Box cameras

#	Parameter	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" Progressive Scan CCD / CMOS
5.	Lens Type	Varifocal, C/CS Mount, IR Correction Full HD lens compatible to camera imager
6.	Lens#	Auto IRIS 8 – 50 mm,
7.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264 individually configurable
8.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)
9.	IR Cut Filter	Automatically Removable IR-cut filter
10.	Day/Night Mode	Colour, Mono, Auto
11.	S/N Ratio	≥ 50 dB
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus
13.	Wide Dynamic Range	True WDR upto 100 db
14.	Audio	Full duplex, line in and line out, G.711, G.726
15.	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.
16.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & G

#	Parameter	Minimum Specifications or better
17.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
18.	Intelligent Video	Motion Detection & Tampering alert
19.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface
20.	Operating conditions	0 to 50°C
21.	Casing	NEMA 4X / IP-66 rated & IK 10
22.	Certification	UL2802 / EN, CE ,FCC
23.	Power	802.3af PoE (Class 0) and 12VDC/24AC

At few places 2.8mm – 11 mm lens would be required depending upon the location of the camera and area to be covered. 2.8mm – 11mm lens requirement can be assumed as 20%. However the actual type of lens required would depend upon the field-specific user requirement & percentages may vary to some extent.

* All of the camera feeds would be used for Video Analytics while about 40 would be used for ANPR (Automatic Number Plate Recognition). Please note that the exact numbers may change depending upon the survey carried out by the successful bidder along with Police Dept. Bidders would be expected to provide necessary provisions in these cameras to support Analytics.

6.8.4. Pan, Tilt and Zoom cameras (PTZ)

#	Parameters	Minimum Specifications or better
1.	Video Compression	H.264
2.	Video Resolution	1920 X 1080
3.	Frame rate	Min. 25 fps
4.	Image Sensor	1/3" OR ¼" Progressive Scan CCD / CMOS
5.	Lens	Auto-focus, 4.3 – 129 mm (corresponding to 30 X
6.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264 individually configurable
7.	Minimum Illumination	Colour: 0.05 lux, B/W: 0.01 lux (at 30 IRE, F 1.2) or better
8.	Day/Night Mode	Colour, Mono, Auto
9.	Wide Dynamic Range	True WDR upto 100 db
10.	S/N Ratio	≥ 50dB
11.	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

#	Parameters	Minimum Specifications or better
12.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, , Electronic Image Stabilization
13.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S & G
14.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption
15.	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.
16.	Intelligent Video	Motion Detection & Tampering alert
17.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface
18.	Operating conditions	0 to 50°C
19.	Casing	NEMA 4X / IP-66 rated & IK10
20.	Power	802.3at PoE+ (Class 4) or 24VDC/24AC
21.	Certification	UL2802 / EN, CE ,FCC

6.8.5. Fisheye camera

Fisheye camera to be provided 360 degree surround view without blind spots while the speed dome to provide fast, precise pan/tilt zoom movement & capture details with precise quality from large distance coverage.

- 5-Megapixel CMOS Sensor
- Maximum frame rate of 30 fps @ 1080p Full HD
- 1.5mm Fisheye Lens for 180 degree Panoramic view & 360 degree Surround view.
- Removable IR-cut Filter for Day & Night Function
- Real-time H.264 MPEG-4 Encoding
- WDR for Visibility in Extreme Bright or Dark Environments.
- Vandal Proof IK 10 rated, NEMA 4x/IP66 rated Housing.
- Built in 802.3af Compliant PoE.
- Built in Micro SD/SDHC/SDXC Card Slot for on board Storage.

6.8.6. Infrared Illuminators

The infrared illuminators are to be used in conjunction with the Fix Box / PTZ cameras specified above to enhance the night vision.

#	Parameter	Minimum Specifications or better
1.	Range	Min. 100 mtrs
2.	Minimum Illumination	High sensitivity at Zero Lux
3.	Angle of illumination	Adjustable

#	Parameter	Minimum Specifications or better
4.	Power	Automatic on/off operation
5.	Casing	NEMA 4X / IP-66 rated
6.	Operating conditions	-5° to 50°C
7.	Certification	UL / CE / FCC / EN

6.8.7. Industrial Grade outdoor PoE switches

#	Parameter	Minimum Specifications
1.	Type	Managed Outdoor switch
2.	Ports	• Minimum 4 10/100 TX PoE • May require higher port density at some locations, depending upon site conditions • May require fiber ports at some locations, depending upon site conditions/distances.
3.	PoE Standard	IEEE 802.3af or better
4.	Protocols	• Support 802.1Q VLAN • DHCP support • SNMP Management
5.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering.
6.	PoE Power per port	Sufficient to operate the CCTV cameras connected
7.	Rating	IP 30 or equivalent Industrial Grade Rating (This is not essential if the switch is placed in equivalent or better junction box / enclosure)
8.	Operating Temperature	0 – 50 degrees C or better

6.8.8. Camera Poles

#	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 (1980)
2.	Height	• 5 Meter OR higher, As-per-requirements for different types of cameras & Site conditions. • Min. height of camera above the ground should be 10 feet
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)

#	Parameter	Minimum Specifications
4.	Bottom base plate	Minimum base plate of size 30 x 30 x 15 cms
5.	Mounting facilities	To mount CCTV cameras, Switch, etc.
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 Section 8.4 (pt. 4)
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.

Type	Sign Design	Remarks
A		To be used at 80% of the Places
B		To be used at select places where text can be read. Text should be in Marathi at majority of places

Type	Sign Design	Remarks
C	 e	This may be used on a select few places in the city, usually on the main pole of the location where multiple cameras are installed. Text should be in Marathi in majority of places.
D		This is an alternative to type C.

6.9. Smart Pole

6.9.1.Specifications

#.	Specifications
1.	Smart pole should able to meet city aesthetic requirement and it should be visually appealing. It should easily blend-in into city street pole master plan.
2.	Should be able to support 1 light arm with maximum height requirement up-to 30 meter.
3.	It should be possible to house minimum 3-4 telecom technologies (GSM, WCDMA, LTE and Wi-Fi etc.) simultaneously. It should also be possible to support future technologies such as 5G & 6G etc.
4.	Site passive infra (space and power) sharing among telecom operators is mandatory requirement.
5.	It should be possible to support LED luminaries from reputed OEMs
6.	Smart Pole shall adhere to the standards for poles (wind speed, climate, aesthetics etc.) and policies governing the Authority or as mandated by regulatory authority of Government of India and Andhra Pradesh.
7.	It should be possible to support connectivity for Smart pole
8.	The maximum allowed diameter (at bottom section) is 250mm
9.	All cabling, cooling/heating etc. should be via/inside the pole and it should not be visible from outside due to aesthetic and security reasons
10.	It should meet EMC requirement of telecom sites as per Indian regulations
11.	The minimum power backup requirement is minimum 2 hrs. for telecom equipment
12.	It should be possible to provide multiple color options as asked by municipality/user as per city light pole colors
13.	It should be possible to house radio units with integrated antenna, MW /optical transmission unit , SMPS (AC to DC convertor), batteries, controllers, power distribution etc. inside the smart pole
14.	It should be possible to house telecom equipment's from all reputed OEMs.
15.	It should be possible to provide light connection in daisy chain with separate MCB for lighting and telecom part
16.	There should be provision to have separate connection for light as well for telecom equipment for maintenance purpose.
17.	The paint material (to cover the RF section) should complied to RF/Telecom requirements
18.	It should be possible to color the complete body (including RF equipment camouflaging) by any paint color
19.	The camouflaging material (to cover RF equipment's) should have RF transparency with maximum 0.5db of attenuation covering all the radio frequency bands available in India

#.	Specifications
20.	The cooling/heating equipment's to cool /heat telecom equipment should be integral part of smart pole. Maximum allowable limit for cooling equipment is 100W for cooling solution, efforts should be made to reduce the power consumption as much as possible.
21.	The smart pole structure should be IP67 up-to 1 meter height from reference ground level.
22.	There should be suitable mounting options for Radio /Antenna unit mounting
23.	The ambient temperature requirement is 0-50 deg
24.	The overall power budget for smart pole should not exceed 2KW (telecom + lights)
25.	It should be possible to support 2 light arm option by smart pole
26.	Underground space should be used for telecom equipment's with suitable telecom grade enclosure box
27.	The minimum life requirement of above smart pole structure is 17 years (metal parts)
28.	The System Integrator should not use any banned /restricted material as per Indian regulations
29.	Pole hat mounting should have suitable option for GPS antenna, small MW antenna
30.	The smart pole should support Environmental sensors

6.9.2. LED based Smart Street light

National Lighting Code by Bureau of Indian Standards (IS)- SP 72, 2010, IS 1944, IS 1977 and IEC Standards shall be complied for design and development of street lighting calculations, selection of lighting fixtures, lighting technologies, pole structure & erection, cable selection and sizing, insulation requirements, conductor specifications etc.

Specifications

The scope includes design, development, manufacturing, testing and supply of energy efficient luminaire complete with all accessories, LED lamps with suitable current control driver circuit including mounting bracket for street light and High mast light. The luminaire shall be suitable for rugged service under the operational and environmental conditions encountered during service.

6.9.3. Smart Street Light Solution

#	Specifications
1.	The smart street lighting system should be able to operate in any weather conditions
2.	Smart street lighting system should be able to communicate to the feeder panel.
3.	The smart street lighting system should be able to communicate to the Lighting Operations Management software hosted on the datacentre

#	Specifications
4.	The smart street lighting system should have the capability to receive the instruction from the Lighting Operations Management software and act accordingly
5.	The smart street lighting system should be able to operate the lights switch on/off, increase/decrease luminosity (Dimming) as per the command received from the Lighting Operations Management software. This control of smart street lights should also be available through a mobile App (compatible with iOS, Android)
6.	The software should have the capability to apply policies to the smart lighting system. Example: set up policies like light up alternate lights during low traffic density, increase the luminosity of the lights as per the dullness of the daylight, scheduling of light functioning etc.
7.	The city administration should be able to see the real time status of the Smart Lighting System on a city map view of the Lighting Operations Management software
8.	The city administration should be able to operate the Smart Lighting System manually too.
9.	The smart lighting system should be able to communicate the system issue or failure to the Lighting Operations Management software.
10.	The smart lighting system are preferably a combination of LED lights
11.	Should enable Over the Air (OTA) firmware update

6.9.4.LED Luminaire

#	Minimum Specifications
1.	High bright white power LEDs shall be used in the Luminaries and the wattage of these LEDs shall be>1W and <3W.
2.	Life span of LEDs used in the Luminaire shall be more than 50,000 hours at 70% light output.(Manufacture shall submit the proof-L70& TM 21 test report)
3.	Color rendering index (CRI) of the LEDs used in the luminaire shall be greater than 70.
4.	Color temperature of the proposed white color LED shall be 5000K-6500K
5.	Junction Temperature; Should be less than value at which LM80 (IS16105) data published. Should be >105 Degree C
6.	The distribution of luminaire illumination (control of distribution) shall be based on type of roads as per BIS standard IS 1944
7.	Power Factor: 0.95
8.	Chip Efficacy: Shall be 135 lumen/watt, system lumen output at 25 degree C, supported by LM80 report shall be submitted.
9.	CRI of Luminaries: >=70 (supported by LM80)
10.	Light Uniformity ratio (Emin / Eavg) shall be as IS 1944 based on category of road
11.	The luminaire light output (lumen) shall be constant. The voltage variations/ fluctuations in the specified voltage range shall not impinge upon the lumen it produce maximum +/-2% is allowed throughout in the input operating voltage range
12.	Operating voltage:

	120 V to 270 V universal electronic driver with surge protection of 6 KV (Application IS 15885, Driver safety 16104-1/2)
13.	Total Harmonic Distortion: <10% THD Test method IEC:610003-2
14.	LEDs shall be operated at a current less than 90% of its rated current
15.	LED driver efficiency: >=350ma<=1000mA
16.	LED driver efficiency Driver (High Voltage, Low current): >85%
17.	Luminaire body temperature should not exceed 30 deg C from ambient (45 deg C) without tolerance of 10 deg. C after 24 Hrs.
18.	Heat dissipation/heat sink: Well-designed thermal management system with defined heat sink
19.	Input Current< 1000mA
20.	Should have Open Circuit protection
21.	The Luminaire shall be equipped with distortion free, clear, heat resistant, toughened, UV stabilized glass cover in the front fixed to the die cast. Aluminum frame which shall be fixed to the housing by means of stainless steel screw.
22.	The Luminaire shall be built in such a way it can withstand wind speed of 80Kmps
23.	Cover/glass without lens or with lens: Fixture cover-UV stabilized Polycarbonate/heat resistance toughened glass or equivalent will be accepted for the Luminaire without lens. For the Luminaire with lens, toughened glass be required with proper IP66 provision
24.	Frequency: 50 Hz+/-3%
25.	Operating temperature: Range -10C to +50 C
26.	Protections: IP66 for all wattage, Surge protection 6 KV, IEC61000-4-5
27.	Working humidity: 10% to 90% RH
28.	Conformation standards of Luminaire: The Luminaire should conform to IEC 60598/IS: 10322. The Luminaire should be tested as per IEC 60598-2-3:2002/IS: 10322 Part 5 sec-3 standards and following test reports should be submitted. Heat resistance test, thermal test, Ingress protection test, drop test electrical/insulation resistance test, endurance test, humidity test, photometry test (LM80 report) vibrant test.
29.	Finish: Aesthetically designed housing with corrosion resistant polyester powder coating
30.	Luminaire configuration/technical requirement: Side entry type. Shall consist of separate optical and color gear compartments. It should be easy replacement in the field condition
31.	Compliance: RoHS/CE/ERTL/ERDI
32.	Surge protection: External surge protection of 10 KV to be separately installed with the each fixture

33.	Lamp starting time: Max 10 sec
34.	Overall system efficacy: >85%

6.9.5. Feeder Panels

The System Integrator shall replace the feeder panel in non-working conditions as per the below mentioned specifications. System Integrator shall upgrade the feeder panels in working conditions (like remote transfer of data) with the below mentioned functionality.

The design and operation of feeder panels shall comply with SP 72 Part 8 of National Lighting Code 2010.

#	Specifications
1.	Principle equipment should be designed on the basis of `Lossless Series Reactance with Secondary Compensation' technology (Auto-transformer)
2.	The efficiency of such principle equipment should not be less than 99.4% between 50% - 110% of loading
3.	Other than basic switching components, no other moving parts are allowed to be installed in the feeder panel
4.	240 VAC 50 Hz Single Phase Two Wire / 415 VAC 50 Hz Three Phase Four Wire Input
5.	Three Taps of Single / Three Phase Four Wire Outputs
6.	Standard Output Taps in each Phase at 200/205/210 VAC @ 240 VAC Nominal Input
7.	Feeder panels should have GPRS/GSM based remote streetlight monitoring system with capacity for self-protection from short-circuit, over voltage and anti-theft alert
8.	The rating of the Streetlight controller should be at least 1.3 times the lighting load as measured during the initial studies
9.	Energy Meters to be installed in separately sealable and open able compartment within the Feeder Panels as per the following specifications: • Energy Meters should have Accuracy class of Class 1 or better; • Meters could be either three phase whole current or CT operated for LT as may be required based on the load connected to the feeder panel. The space to be created in the feeder panel for housing the meters should consider the same. • Energy Meters should be capable of logging parameters for each 15 minute time block with stamping of date and time. Such data logs should be retained in the energy meters for a period of 60 days or more. • Such Energy Meters should record the following minimum parameters • Phase to neutral voltages o Phase-wise current o Phase-wise power factor and frequency o Total active power o Total reactive power o Total active energy o Total reactive energy o Total KVAH energy • Meters should have requisite port (Serial port communication – RS232 or RS485) for enabling remote reading and for connection of Modem for the same o Energy Meter specifications should meet the minimum specifications specified by POWER DISTRIBUTION COMPANY and a sign-off on the same

#	Specifications
	shall be obtained from POWER DISTRIBUTION COMPANY prior to finalizing the specifications; o Energy Meters shall be tested, installed and sealed in accordance with procedures specified by POWER DISTRIBUTION COMPANY; o A signoff from POWER DISTRIBUTION COMPANY on the design and specifications of the compartment in the Feeder Panel where the meters are to be housed is also recommended;
10.	Bidder has to install appropriate power conditioning devices to protect the new EE technologies and components of feeder panels from damage. Poor power quality is not allowed as an excuse for non-functioning of the new technologies installed under the project
11.	Fixed capacitor with appropriate capacity shall be introduced in each feeder panel to always maintain a power factor above 0.90
12.	In case of Single phase controller unit, 1 pole contactor or multiple parallel pole contactors should be used and in case of 3 phases, appropriate duty 3 pole contactor should be used. The number of contactors used should be suitable for ON/OFF/Dimmed and for changeover between full voltages to various voltage taps and interchanging between taps. The panels should be equipped with a microprocessor based Dual Channel Almanac Timer controller which should be user programmable to enable setting of ON/OFF/Dimmed times and also switching over to savings mode/bypass mode when required
13.	All the principle equipment's along with input output switchgears, metering, switches (bye pass and tap changers), contactors, fuses, auto transformer coils etc. should be of reputed manufacturers and should meet best engineering practices and norms as applicable in relevant standards; • Auto transformer coil should have full current operating efficiency of better than 99% • The total heat dissipation from single coil should not exceed 6 watts-sec/kVA under fully loaded condition • The rated current of the auto transformer should be for continuous 120% that of input rated current • The switched fuse units should be of 32 Amp continuous AC current capacities. • Fuses used should be of 20 Amp. Rating of high rupturing capacity (S/c current at least 50 kA)
14.	The bidders should always ensure that the System is capable to capture live data and record it at variable time-intervals. Following parameters should be recorded for every 60-120 minutes time interval: • Voltages • Current • Power Factor • Active Power (kW) • Apparent Power (kVA) • Metering kWh cumulative • Metering kVAh cumulative • Number of hours the lamps were glowing • Special emergency on/off facility with wireless control. • Benchmarking capacity so as to generate alert SMS for: o Phase-wise currents on crossing threshold values o Phase-wise voltages on crossing threshold values o JSCLB trips o Theft alerts

#	Specifications
	○ Group failure of lights ○ Contactor failure ○ No output supply • Alert SMS shall be forwarded to five (5) phone numbers. • GPRS/GSM modem should be used
15.	Enclosure Box of feeder panels shall be IP-56 compliant and should be fabricated out of MS sheet SWG 16 / 14 duly powder coated for corrosion resistance and long life. • It should have Single Phase power socket for connecting utility tools like drill machine etc. (capacity 1phase 240Vac / 5Amp socket) • Utility Service Lamp inside Panel for use during maintenance work • Gland Plates for Cable Entry at Incomer and Outgoing • Auto Bypass / Tap Changing in lieu of Manual. The tap changing should be automatic between the full voltage and lower voltage for minimum two numbers selected taps.
16.	The bidder shall have to get the control panels fabricated from the vendor having type test certificate from CPRI for 31 MVA short-circuit rating up to 400 amp for cubical panels. The copy of the type test certificate shall also have to be produced failing which feeder panels shall not be accepted
17.	Design life of the control panel should be mentioned in form of MTBF (mean time between failures) and it should be minimum 15 years

6.9.6. LED Luminaire Controller

#	Specifications
1.	Advance 32 bit Microcontroller based design.
2.	Very easy key board operation
3.	HMI LCD display. 16 character and two line type display. Which help while maintenance and reduce dependability. Contentious Scrolling display of events (Like ON time, Off time, Dimt time, Voltage, Current, Staggering time , Alarm events, Burning hours, etc.) on Single HMI LCD display to help the local monitoring of systems. Parameters can be updated from local panel. Log the alarm of last 5 events
4.	Data Measurement for Monitoring and controlling Data monitoring through Class 1 type Multi – Function Panel mounted Energy meter : By using this to measure the individual phase voltage, individual phase load amps, PF, KW, KVA, KVAR, Phase to Phase voltage, Average PF, KWH etc. (Local display of 36 and 28 for remote display in software)
5.	Auto / Manual facility by way of contactor / relay operation for faster service mode. From local panel in manual mode it shows individual line / channel current and show no of lamp which is not working which helps to judging the problem in line (by difference of calibration current and existing line current. Judgment is possible for approximately find out no of lamps are not working
6.	Street light ON / OFF / Dim on Longitude, Latitude base sunset and sunrise time generation not by any fixed time table
7.	Door Open information
8.	Real time clock with battery with life of more than 7 years (Manufacturer provided 10 years life for the battery with the accuracy of +/- 60 second per month. Power reserve of more than 60000 hours)
9.	System parameter data protection with special RAM, which hold the parameter for more than 10 years without any power
10.	Master and user Password Protection.

#	Specifications
11.	Inbuilt auto recovery systems for power failure which helps in streetlight operation
12.	Double Inrush current capability of electrical switch gears to support sodium vapor lamp

6.9.7. Centralized Management Software

#	Specifications
1.	Web Base Software replaces visual inspections of individual street lighting while sitting at workstation with Internet connectivity. Also by fault alarm and monitoring of data user can judge the fault status and severity of fault
2.	Remote switching through Web Base Software to override local controller
3.	User can demand any time live status of feeder pillar for current electrical and real time parameters
4.	Emergency Stop / Manual ON / Manual OFF / Test Mode of feeder pillar
5.	User can monitor and change all settable parameter setting and clock time setting
6.	Control at any level of individual Street lights. Generate electrical profile of any individual feeder pillar
7.	Unit should be directly mapped on GIS Map
8.	The software shall receive the self-generated data message from individual Feeder Pillar like, ON time, Off time, Dim time, Power Down time, Auto mode / Manual Mode, Volt Fault, Over Current Fault, Short Circuit Fault, Neutral Fault, RTC Fault, ADC Fault, Memory Fault, Low Ampere Fault, Door Open, Relay Fault, Calibration Data and acknowledgement of massage demand by WEB of Parameter writing, E Stop, Test Mode, E Profile. All these messages contain all electrical parameter with real-time clock date and time
9.	The software shall generate report of any date or any date range for fault and message of individual unit or all the units. The software shall also generate Range Report for fault, Message, Voltage graph, Current Graph, Streetlight On time, VA Consumption, etc.
10.	All the data collected by the software shall be exported to work sheet format for further analysis as per requirement. The system should be able to generate graph and reports as per requirements
11.	Can be operated and viewed from anywhere in the world
12.	System should be easily expanded and maintained. The system should have the capabilities for new configurations remotely.
13.	Web Interface should give instant status of the street lights on the dynamic Google map

6.9.8. Minimum Illumination Level

#	Type of LED Luminaries	Vertical Distance from the floor level (Meters)	Minimum Illumination Level (Lux) centre	Color of Illumination
1.	45-50W	5	(12-15)	5000K-6500K
2.	100-105W	7	(15-18)	5000K-6500K
3.	140-170W	7	(18-20)	5000K-6500K

4.	260W	7	(20-22)	5000K-6500K
5.	50W	5	(12-15)	5000K-6500K
6.	105-110W	7	(15-18)	5000K-6500K
7.	190W	7	(20-22)	5000K-6500K
8.	25-30W	5	(10-12)	5000K-6500K
9.	60W	7	(15-18)	5000K-6500K

6.9.9. Minimum desired illumination levels during peak hours

#	Type of LED Luminaries	Type of Road	Lamp mounting height from the floor level (Meters)	Minimum Illumination Level (Lux) centre	Color of Illumination
1.	250-260W		Above 18	(20-22)	5000K-6500K
2.	190W	A1	Between 11-15	(20-22)	5000K-6500K
3.	140-170W	A1	9-15	(18-20)	5000K-6500K
4.	90-120W	A2/B1	7-9-11	(15-18)	4300K-5600K
5.	70-120W	A2/B1	7-9-11	(15-18)	4300K-5600K
6.	70-120W	B1/B2	6-7-9	(15-18)	4300K-5600K
7.	70-50W	B1/B2/C1	7-9	(12-15)	4300K-5600K
8.	45-50W	B1/B2/C1	5-7	(12-15)	4300K-5600K
9.	25-30W	B1/B2/C1	5-7	(10-12)	4300K-5600K

- Variation in illumination level shall be ± 2% is allowed in input voltage range from 180VAC to 250VAC.
- The illumination shall not have infra-red and ultra-violet emission. The test certificate from the NABL approved laboratory shall be submitted.
- Electronic efficiency shall be more than 85%

6.9.10. Conformance Standards

Product Certification should be obtained from UL or CPRI or any other NABL certified lab. The following test reports should be provided:

LM-79	Luminaire efficacy (Photometry data)
LM-80	LED chip data
IP 67	Luminaire Ingress Protection
Luminaire Endurance Test	Practical testing of luminaire through 20,000 cycles
EN 60929	Performance
IEC 60598-1	General requirement and tests

IEC 61000-3-2	Limits for Harmonic current emission - THD < 10%

6.9.11. Environmental Sensors

Functional Specifications

j) Smart environment sensors will gather data about pollution, temperature, rains, levels of gases in the city (pollution) on a daily basis. It is for information of citizens and administration to further take appropriate actions during the daily course / cause of any event.

k) The environment sensors should have the following capabilities:

- They should be ruggedized enough to be deployed in open air areas, on streets and parks
- They should be able to read and report at least the following parameters: Temperature, Humidity, Ambient Light, Sound, CO, NO2, NOX, CO2, SO2.

l) Smart environment sensors will enable citizen to keep a check on their endeavors which impact environment and enable the city to take remedial action if required. These environmental sensors shall be connected via wireless/wired network.

m) The data should be collected in a software platform that allows third party software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.

n) The sensor management platform should allow the configuration of the sensor to the network and also location details etc.

o) The environment sensors will be deployed on the smart poles measure and log the data to be transmitted to the Integrated command and control centre

Technical Specifications

#	Parameter	Specification
11.	Measurement principle	• Temperature, Humidity, CO, NO2, NOX, CO2, SO2
12.	Measurement component Measurement range	• NO2: 0 to 10 ppm • NOX : 0 to 50ppm , 5000ppm • SO2 : 0 to 500 ppm • CO : 0 to 50ppm, 5000ppm • O3: up to 1000 ppb • CO2 : 0 to 10% / 0 to 20% • PM 2.5: 0 to 230 micro gms / cu.m • PM 10: 0 to 450 micro gms / cu.m • UV: up to 15 mW/ cm2

13.	Repeatability	• ±0.5% FS
14.	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
15.	Temperature and Humidity Sensor	• Real-time Temperature Range: Indoor -10ºC ~ +70ºC (+14ºF ~ +122ºF) • Real-time in Air Humidity Level Display (up to 100%)
16.	Span drift	• ±2.0% FS max./week • ±2.0% FS max./month for O2 meter
17.	Response speed	• 120 seconds max. for 90% response from the analyzer inlet
18.	Connectivity (Minimum)	• Ethernet connectively

6.9.12. Public Internet Access Specifications

WLAN Controller

#	Parameter	Specifications
1.	Hardware	Redundancy Features: Controller must support Active: Active and Active: Standby. Same license should be shared by both the controller.
2.		WLC should be dedicated appliance with support for up to 100 Access points. Should be in High Availability mode. Should have 2 nos. of 100/1000/10Gig ports
3.	General Feature Requirements	Full web based real time NMS system to monitor services working.
4.		Full capability for EAP/SIM, EAP/AKA etc. Mobile Data Offload to be done with Mobile Operators.
5.		To allow LSCL to download/ view performance of services utilised by subscribers with key information of Username, MAC, IP, Location, Duration, Upload/ Download & Disconnection reason
6.		Multiple payment gateway integration required so subscribers can make the payments using online/ offline mode, including prepaid mobile balance & wallet applications
7.		Advertising platform integration -AAA to support advertisements from multiple parties
8.		IOS & Android Applications to be given for seamless connectivity to network –auto detect/auto login
9.		Content delivery support

10.		Bidder should share usage data analytics from all monetization across all SSID's with LSCL on a monthly basis
11.		Ability to map SSID to VLAN
12.		WLC Should support Rogue AP detection, classification and standard WIPS signatures.
13.		Should support automatic channel selection – interference avoidance (Co-channel management, Adjacent Channel Management, Channel reuse management)
14.		Should provide Mesh capability for Mesh supported AP
15.		For smooth, seamless and easy manageability, operation, interoperability and maintenance, the bidder should offer/quote WLC & WAPs of the same make (OEM).
16.		Controller should support deep packet inspection for all user traffic across Layer 4-7 network
17.		Support 802.11a/b/g/n/ac wireless standards
18.	AP to Controller Communication	Use of industry standards-based (IEEE or IETF) tunneling protocols; specify standard that the tunneling mechanism is based on.
19.	Auto Deployment of APs at different locations	Access points can discover controllers on the same L2 domain without requiring any configuration on the access point.
20.		Access points can discover controllers across Layer-3 network through DHCP or DNS option
21.	Firewall & IPS	Built-in ICSA Certified Wireless Firewall in the Switch
22.		Firewall should support minimum 100000 concurrent sessions
23.		System should provide L2 / L3 stateful firewall, Role based firewall, DOS attacks and Storm control
24.		Should support Access Control Lists (ACLs).
25.		The firewall must be able to take action including allowing the traffic, denying the traffic, rejecting the traffic, routing the traffic, destination or source NAT the traffic, modify the QoS level of the traffic, and blacklist (remove from the network) the client for policy matches
26.		Should include IPS licensing for 3 years from the date of installation
27.		Should adhere to the strictest level of security standards, including 802.11i Wi-Fi Protected Access 2 (WPA2), WPA, Wired Equivalent Privacy (WEP), 802.1X with multiple Extensible Authentication Protocol (EAP) types, including Protected EAP (PEAP), EAP with Transport Layer Security (EAP-TLS), EAP with Tunneled TLS (EAP-TTLS).
28.	System Architecture	Centralized MAC addresses filtering
29.		Should support onboard and external DHCP server
30.		Controller should support Onboard AAA server

31.		Radio coverage algorithm must allow adjacent WAPs to operate on different channels, in order to maximize available bandwidth and avoid interference
32.		Support roaming between access points deployed on same subnet and different subnets
33.	QoS features	Per user bandwidth Rate Limiting
34.		Self-healing (on detection of RF interference or loss of RF coverage)
35.		Should support per user, per device, and per application/TCP-port prioritization
36.		Should support 802.11e WMM
37.		Support advanced multicast features with multicast rate optimization, multi-channel use and IGMP snooping
38.	RF Management	Traffic shaping capabilities to offer air-time fairness across different type of clients running different operating systems in order to prevent starvation of client throughput in particular in a dense wireless user population without the use of client specific configurations or software.
39.		Load balancing across bands and steering of dual-band capable clients from 2.4GHz to 5GHz in order to improve network performance without the use of client specific configurations or software.
40.		Allow for automatic and manual RF adjustment.
41.	Inline Security Features	Should allow authenticated client devices to roam securely from one access point to another, within or across subnets, without any perceptible delay Security during re association.
42.		Controller should support DES, 3DES and AES-128 and AES-256 encryption, with site-to-site and client-to-site VPN capabilities; should have provision to supports IPSEC tunnels
43.	Management	Command line interface to control and manage all aspects of the WLAN system from controller
44.		SNMP v3 or latest
45.		Browser-based system for total solution management including: configuration, monitoring, troubleshooting
46.		Single dashboard view of overall network, user, and security status

Outdoor Access Point

#	Parameters	Specifications

1.	External Protection	The Access point shall be IP66/IP67 rated for dust and water Ingress protection. Third party casing will not be accepted.
2.	Features	Must support the ability to serve clients and monitor the RF environment concurrently.
3.		Access Points proposed must include radios for both 2.4 GHz and 5 GHz.
4.		Should support mesh capabilities for temporary connectivity in areas with no Ethernet cabling.
5.		Mesh support should support QoS for voice over wireless.
6.		should support 802.11e and WMM
7.		Must support Reliable Multicast Video to maintain video quality
8.		Must support QoS and Call Admission Control capabilities.
9.		Must support IPv4 and IPv6.
10		
11		Must support telnet and/or SSH login/Console to WAPs directly for troubleshooting flexibility.
12	Ports	AP should have minimum two Auto-sensing Gigabit Ethernet port.
13		Must support Power over Ethernet.
14	Throughput	Must support data rates upto 1.3Gbps on 5Ghz radio.
15	Power	Must support Direct 100- 240 VAC / DC / PoE+ to power up access point.
16	Mobility	Minimum of 16 SSIDs available on each AP simultaneously without negatively impacting system performance
17		Access Point radio should be minimum 3X3 MIMO with minimum 3 spatial streams or more. Dual Radio capable.
18	Security	Capable of multi-function services including: data access, intrusion detection, intrusion prevention, location tracking, and RF monitoring with no physical “touch” and no additional cost
19	Management	Real-time, fully integrated spectrum analyzer capabilities on the APs, that does not require dedicated sensors or separate operating system running on the AP radios.
20		The Access Point should have the technology to improve downlink performance to all mobile devices.
21	High throughput	Access Point should be 802.11ac ready from day one.
22	Diagnostics	Real time packet capture on the APs, without disconnecting clients.

23	Mounting	Access point should be supplied with OEM mounting kit and shall support pole, wall, and roof mounting options
24	Operating Temperature	The Access point shall be rated for operation over an ambient temperature range of 0° to 60°C
25	Transmit Power	Must support up to 23dbm of transmit power for 2.4 & 5Ghz radios, (limited as per Govt, of India regulation for such WAP)

L2+ 8 Ports Managed Switch

#	Parameter	Specifications
1.	Port Density & Redundancy	The switch should have 8 ports 10/100TX and with 2 combo ports (10/100/1000T or 100/1000 SFP)
2.	System Capacity	Should have 16MB flash memory, 16K MAC addresses, 128MB RAM
3.	Performance	The switch should have min. 5.6 Gbps of switching capacity & min. 8 Mbps of forwarding rate
4.	VLAN	Support for Port-based VLANs, 4096 VLANs (IEEE 802.1Q), GARP VLAN Registration Protocol (GVRP), MAC-based VLANs, Port-based Private VLANs, IP subnet-based VLANs 256.
5.	Quality of Service	Support for Egress rate limiting, Eight egress queues per port, Voice VLAN, DSCP for IP-based QoS, Differentiated services architecture, IEEE 802.1p Class of Service with strict and weighted round Robin scheduling.
6.	Multicast	Support for IGMPv1 and IGMPv2 snooping, Multicast groups 255, IGMPv2 snooping querier
7.	Management	Support for Telnet server, should have Console management port, Web GUI, Enhanced Stacking, HTML, HTTP, TFTP, zModem, SNMP V3, RMON 4 groups Stats, History, Alarms and Events, Event log, Auto config, MIB, SNTP, sFlow or equivalent.
8.	Security	The switch should support TACACS+, RADIUS accounting and RADIUS client, IEEE 802.1x port-based Network Access Control (NAC), IEEE 802.1x multiple supplicant mode, EAP, EAP-TLS, LEAP, PEAP, TTLS, Microsoft NAP compliant, Symantec NAC support, Per port MAC address filtering, Layer 2/3/4/ Access Control Lists (ACLs), SSLv3 for Web management, Per port MAC address limiting, MAC address security/lockdown, Guest VLANs and SSH session Time out.
9.	Resiliency	IEEE 802.1D Spanning-Tree Protocol, IEEE 802.1D-RapidSpanning-Tree Protocol and IEEE802.1q-Multiple Spanning-Tree Protocol, BPDU guard, Loop guard and Root guard
10.	Other Essential Feature	Support for IPv6 host, ICMPv6, IPv6 ACL, Dual-stack IPv4/IPv6 management, IPv6 applications WEB/SSL, Static IPv4 routing 4K,

		RIPv1,v2, Proxy ARP, IEEE 802.3ad, ICMP, LLDP-MED, LLDP, DHCP snooping, DHCP option 82, DHCP relay, ICMP. The switch should have ECO Friendly design and fan less operation.
11.	Power Characteristics	Voltage: 100-240V AC (10% auto-ranging), Frequency 47-63Hz Operating temperature: 0C to 40C Storage temperature: -25C to 70C Operating humidity: 5% to 90% non-condensing
12.	Safety Certifications	EMI: FCC class A, EN55022 class A, C-TICK, VCCI Class A, CE, UL 60950-1 (cUlus), EN60950-1 (TUV), EN60825 Etc and Compliant with RoHS standards.

L2+ 8 Ports Managed PoE Switch

#	Parameter	Specifications
1.	Port Density & Redundancy	The switch should have 8 ports 10/100TX PoE+(min. 6 Port IEEE802.3at Or 8 Port 802.3af) and with 2 combo ports (10/100/1000Tor 100/1000 SFP) and PoE Power will be min 185W
2.	System Capacity	Should have 16MB flash memory, 16K MAC addresses, 128MB RAM
3.	Performance	The switch should have min. 5.6 Gbps of switching capacity & min. 8 Mbps of forwarding rate
4.	VLAN	Support for Port-based VLANs, 4096 VLANs (IEEE 802.1Q), GARP VLAN Registration Protocol (GVRP), MAC-based VLANs, Port-based Private VLANs, IP subnet-based VLANs 256.
5.	Quality of Service	Support for Egress rate limiting, Eight egress queues per port, Voice VLAN, DSCP for IP-based QoS, Differentiated services architecture, IEEE 802.1p Class of Service with strict and weighted round Robin scheduling.
6.	Multicast	Support for IGMPv1 and IGMPv2 snooping, Multicast groups 255,
7.	Management	Support for Telnet server, should have Console management port, Web GUI, Enhanced Stacking, HTML, HTTP, TFTP, zModem, SNMP V3, RMON 4 groups Stats, History, Alarms and Events, Event log, Auto config, MIB, SNTP, sFlow or equivalent.
8.	Security	The switch should support TACACS+, RADIUS accounting and RADIUS client, IEEE 802.1x port-based Network Access Control (NAC), IEEE 802.1x multiple supplicant mode, EAP, EAP-TLS, LEAP, PEAP, TTLS, Microsoft NAP compliant, Symantec NAC support, Per port MAC address filtering, Layer 2/3/4/ Access Control Lists (ACLs), SSLv3 for Web management, Per port MAC address limiting, MAC address security/lockdown, Guest VLANs and SSH session Time out.

9.	Resiliency	IEEE 802.1D Spanning-Tree Protocol, IEEE 802.1D-RapidSpanning-Tree Protocol and IEEE802.1q-Multiple Spanning-Tree Protocol, BPDU guard, Loop guard and Root guard
10.	Other Essential Feature	Support for IPv6 host, ICMPv6, IPv6 ACL, Dual-stack IPv4/IPv6 management, IPv6 applications WEB/SSL, Static IPv4 routing 4K, RIPv1,v2, Proxy ARP, IEEE 802.3ad, ICMP, LLDP-MED, LLDP, DHCP snooping, DHCP option 82, DHCP relay, ICMP. The switch should have ECO Friendly design and fan less operation
11.	Power Characteristics	Voltage: 100-240V AC (10% auto-ranging), Frequency 47-63Hz Operating temperature: 0C to 60C Storage temperature: -25C to 70C Operating humidity: 5% to 90% non-condensing
12.	Safety Certifications	EMI: FCC class A, EN55022 class A, C-TICK, VCCI Class A, CE, UL 60950-1 (cUlus), EN60950-1 (TUV), EN60825 Etc and Compliant with RoHS standards.

Network Management System and WLAN Management System

#	Network Management System for LAN Switches
1	Management system should provide a single integrated solution for comprehensive lifecycle management of the wired and wireless LAN (of same OEM), and should support rich visibility into end-user connectivity and application performance assurance issues
2	The NMS should support an open database schema, configuration, administration, monitoring and troubleshooting of Switches, guided workflows based on best practices with built-in configuration templates, the capability to view the network topology, Layer 2 Services and Fault Management
3	The NMS should automatically discover IP devices, SNMP compliant network devices on the network
4	The NMS should support Inventory management of Network devices, should support Monitoring and troubleshooting of Devices, should support configuration management and reporting.
5	The NMS should support flexible reporting for inventory, user tracking, compliance, switch port usage and end-of-sale
6	The NMS should provide on dedicated appliance/installed as a virtual appliance/ Intel based severs/ AMD based server and should support installation on Windows/ Linux
7	Support for Wireless Management Features (Same functionality can be provided via separate Wireless management system but same should be able to integrate with Wired Management system to implement unified policies)
8	Must show location information of clients, infrastructure Access Points, Rogue Access Points, and RF tags in a map format.
9	Must support following features

#	Network Management System for LAN Switches
10	Wireless LAN Planning and Design, Network Monitoring and Troubleshooting, Indoor location monitoring capability, Centralized Software updates, Network mapping with floor plans for easier automated site survey
11	Shall provide in-depth visibility of finding, classifying, correlating, and mitigating interference from Wi-Fi and non-Wi-Fi sources such as rogue access points, microwave ovens, Bluetooth devices, and cordless phones.
12	Should provide deep integration with the authentication; authorization, posture & Profiler to further extend the visibility across security and policy- related problems, presenting a
13	Must support virtualization, whereby wireless resources (APs, controllers, geographical areas) can be divided into logical domains and administrator access limited to specific
14	NMS has to be from the same OEM as of Switches

Junction Box

#	Parameter	Minimum Specifications
1.	General Requirement	All the junction boxes shall be out door type with IP65 protection from rain, water. Provision for theft prevention. (Expected outdoor temperature 500C).
2.		1.5 mm steel sheet, profiled frame construction consisting of 9 folded rolled hollow sections punched on a 25mm DIN Pitch pattern with load carrying capacity of 1000 Kgs. Front and rear 2 mm thick sheet steel door with PU Foamed Seal (Gasketing) with removable galvanized rectangular frame with holes on a 25 mm DIN pitch pattern with 3 point locking system. The hinges and retainers should be made of die cast, copper nickel chrome plated with SS hinge pins. The doors should be swapped to LH if required with door opening angle 130 deg to VDI. Top panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) boltable from inside. Bottom panel made of 1.5 mm thick sheet steel with PU foamed (Gasketing) with provision for fixing 4 nos of PG 29 glands. Side panels in double walled construction with air gap of minimum 20 mm between two walls with PU foamed(Gasketing) for IP 55 protection. Painting: Electro-phonetic dip coat priming to 20 Microns and then powder coated to RAL 7035 textured Pure Polyester (PP) to 80 to 120 Microns. Powder coated with surface finishing With nano-coating, for the best possible surface protection and corrosion resistance. Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet.
3.		Should be outdoor type, Floor mounting with 3 point locking option, suitable to mount the switches and required UPS. The opening lever/handles shall be made of metal. Each Cabinet will be mounted on a raised height concrete Plinth, 600 - 1000 mm high, as per site requirements
4.		The cabinet will be provided with a dimension of 800mmW x 1200mmH (24UH) x 800mmD with 19" mounting arrangement suitable for the mounting of the associated network, power, UPS and Split Battery components securely and safely within the cabinet.
5.		The junction box shall have floor mount type with required mounting accessories to provide a flexible solution for space constrained traffic applications.
6.		2 x 5 way/15 Amp PDU's will be provided to support the site equipment. 2 x thermostat controlled 230V AC Fans with 100% Duty Cycle with Filter and 2X Filter units with IP55 Rating with rain Canopy shall be fitted to the front door of the cabinet to provide ventilation to cool the equipment. Fan and Cabinet should

		be from same OEM for better SLA and provision to drive power for the camera is required.
7.		75mm Rain canopy on Top with all around projection of the enclosure such that that rain water, water logging shall not penetrate in the junction box and hamper working of the system, cable entry with glands
8.		Small Junction box for mounting the electric meter with viewing window should be provided for mounting Electrical Meter and Fuse and MCB with separate lock for utility power connection, as per electricity board, rules.
9.		Protection from ants, bugs and other small insects entering into the enclosure
10.	Standard and Support	Regulatory Standard Compliance: IP55 to EN60529/09.2000, ISO 9001, 14001, 18001 comply with EIA 310, DIN 41494 and IEC 297 standards. The system should not be an end of life / end of service product.

Field UPS

#	Parameter	Minimum Specifications
1.	Capacity	1 KVA
2.	Input Range	Voltage Range 155-280 V on Full Load Voltage Range 110-280 V on Less than 70% Load Frequency 50 HZ ±3 HZ
3.	Output Voltage & Waveform	220V AC/ 230V AC/ 240V AC (Selectable)
4.	I/P & O/P Power Factor	0.9 or higher power factor
5.	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand
6.	Frequency	50 Hz +/- 0.5% (free running), Pure Sine wave
7.	Crest Factor	min. 3:1
8.	Third Harmonic Distribution	< 3%
9.	Input Harmonic Level	< 10%
10.	Overall Efficiency	Min. 90% on Full Load;
11.	Noise Level	< 55 dB @ 1 Meter
12.	Backup	at least 240 minutes (4 hours / VAH)

13.	Warranty	3 years with UPS & battery
14.	Certification	ISO 9001:2008 & ISO 14001 certified
15.	Protection	To be provided for overload/ short circuit; overheating; input over/under voltage; output over/ under voltage.
16.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection
17.	Interface	SNMP interface support (for remote monitoring)
18.	Galvanic Isolation	To be provided through Inbuilt transformer
19.	Compatibility	UPS to be compatible with DG Set supply and mains supply
20.	Bypass	Automatic Bypass Switch
21.	Technology	True ON-LINE (Double Conversion) with IGBT based inverter and PWM Technology
22.	Support	The system should not be an end of life / end of service product
23.	Operating Temperature	0 to 55 Degrees Centigrade

6.10. ICT Enabled Smart Solid Waste/Bin Management

6.10.1. Overview

Authority is responsible for collection, segregation, transportation, dumping and processing of the city waste from door to door. Authority has deployed vehicles for collection of door to door waste and dumping into the bins/collection points at strategic locations. From these bins/collection point separate 4 wheelers (loaders) carries the waste to the single location called waste processing plant. Also, Authority has field staff which is responsible for street sweeping and collection of street waste and dumping to the nearest bins/collection points.

Currently, managing the people responsible for the activity and proper utilization of assets/resources assigned to them has become a complex job for Authority. The main problems of the existing solid waste collection process are:

[1. Lack of information about the collecting time and area.

2. Lack of proper system for monitoring, tracking the vehicles and trash bin that have been collected in real time.
3. There is no estimation to the amount of solid waste inside the bin and the surrounding area due to the scattering of waste.

4. Physical visit required to verify employee performance

5. The waste keeps lying unattended for several days.

6. There is no quick response to urgent cases like truck accident, breakdown, long time idling etc.]

Authority intends to implement a GIS/GPS enabled Solid Waste Management System practices within the existing landscape to:

1. Manage routes and vehicles dynamically through an automated system.
2. Real time manage of missed garbage collection points
3. Efficient monitor and manage of waste collection bins
4. Do Route optimization which shall help in reduction of trip time, fuel saving and serving more locations
5. Reduce the human intervention in monitoring process
6. Keep history of vehicle routes, attended sites and other details
7. Integrate the dumping ground and transfer station facilities with the centralized locations
8. Reporting of vehicles, garbage collected and other SWM details to higher authorities from any location at any time
9. Monitor and track the activities of field staff force on daily basis

6.10.2. Scope of Work

1. Total No. of waste collection vehicles – 50
2. Total No. of Bins – 50
3. Total No. of Loaders – 10
4. Total Field Staff of Authority (PAN City) –

6.10.3. Details of Work

1. **Business Solutions**

The SI shall be responsible for Supply, Design, Development, Testing, Implementation , Operation and Maintenance (5 years) of ICT based Solid Waste Management System which includes:

ICT Interventions	Key Features
Solid Waste management System	a. GPS tracking of the waste pick up vehicle for real time tracking b. Route Optimization which shall help in reduction of trip time, fuel saving and serving more locations c. Manage routes and vehicles dynamically through an automated system d. Efficient monitoring and management of waste collection bins e. Attendance Management System - Field Staff f. Ensure complete coverage of door to door and community collections served by vehicles g. Monitor and track other municipal corporation vehicles under Solid Waste Management Dept. h. Record history of vehicle routes, attended sites and other details i. RFID devices with vehicle and RFID tagging of Bin to ensure serving by requisite vehicle j. Weight & Volume Sensor based bin to indicate maximum utilization status and trigger vehicle pick up k. Alert / Alarm management - Real time management of missed garbage collection points l. Monitoring & Reporting Application - reports of vehicles, garbage collection status, bin status etc.

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards.

- **Automated Vehicle Locator Management System –**

Web Based Vehicle Tracking and Monitoring Application customized to meet the functional requirements of the solution is envisaged. Authority intends to implement the Automated Vehicle Locator Management System with requirement of customized dashboard specific for monitoring and tracking of solid waste management activities and integration with the RFID system & weight and volume sensor system for bin collection management. The application shall be hosted in the City Operation Center. The application shall leverage on the advanced GPS and GIS technologies for route scheduling, route monitoring, reporting and providing a quick dashboard.

- **RFID based Bin Management System –**

The waste collection vehicles shall be fitted with RFID readers. The RFID readers identify the RFID tags installed in the each of the collection Bins and read the Bin details. This data shall be transferred through the GPS device unit GSM/GPRS connectivity to the integrated application. The RFID readers shall be integrated to the vehicle GPS device unit to achieve this functionality.

- **Weight & Volume Sensor Management System –**

The weight sensors shall be placed at the fixed location over which Bin shall be placed every time it being served by the waste collection vehicle. The weight sensor shall sense the level of occupancy of the bin placed above and trigger alert signal to the city operation center application through GPRS/GSM network.

Volume sensor shall be placed at the fixed location over Bin. When the volume of occupancy (waste) reaches to a particular threshold value, an alert/SMS shall be sent to the concerned person through GSM modem.

- **Mobile GPS based Staff Attendance Management System –**

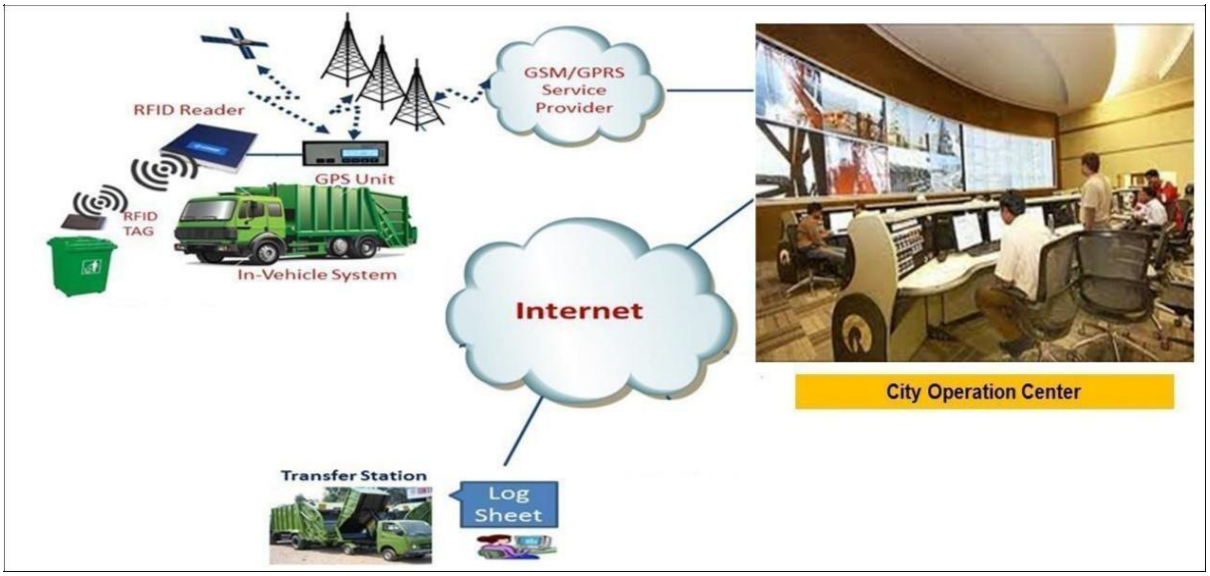
GPS based mobile device shall enable Authority's field staff to register their attendance/presence throughout the day. The system shall periodically track the location (with time stamping) of the staff through their GPS based mobile device and shall map it in the system with the pre-defined area coordinates. The device shall feed the data through GPRS/GSM network to the Command & Communications Center central application for reporting generation and alerts.

2. Infrastructure Solutions

The SI shall be responsible for the supply, installation & commissioning of the following field equipment's as per the technical specifications mentioned in the RFP document:

a. GPS Tracking System with all fittings & fixtures in all the vehicles
b. RFID device installation in all the vehicles & loaders and RFID tagging of all the Bins
c. Mobile biometric device for workers
d. Weight and volume sensors installation at collection point/ bin

ICT Based Solid Waste Management System Schematic Solution Overview



Functional requirement for the sensors shall be as under:

Sr.#	Category	Functional requirement
1	Communication	GSM/GPRS or 3G/4G, Wi-Fi, or better communication technology.
2	Software	Software should have: a. Over the Air programming interface for real time program flashing b. Mechanism to change threshold parameters, through remote access c. Data uploading support over standard TCP/IP based protocols d. Support for network and data security e. Configurable sensor periodicities to conserve power
3	Environmental Protection	Compliance to IP67 standard
4	Operating Conditions	Shall comply with all weather conditions.

6.11. City Bus Intelligent Transport System

Overview

Public transport should always be the hallmark of a good transportation system for a city or a state. The role of public transport is vital, particularly to reduce the use of personalized transport. This system should be such that it can work in co-ordination with the existing transportation systems. An efficient mass transportation system is very much needed for sustainability of not only the economy but also for reducing stress due to pollution on the environment.

Public transport management would need to follow a few fundamentals.

1. Easy access to passengers
2. Passengers feeling secured, when riding the transport
3. Cleanliness

The architecture drawn for the same, should consider the entire eco-system. Few of them could be:

1. Security (both IT and Infra security) – On the move and while at the depot
2. Regular maintenance of the buses.
3. Comfort and security to the stakeholders associated

The bus transport's business SLA's should be properly mapped by the ICT infrastructure SLAs. There are 2 primary segments of the System:

1. Management of the buses
2. Management of the transport infrastructure.

Management of the buses include:

- Cameras focusing inside the bus
- Passenger information system (PIS) inside the bus and outside(front, rear and middle)
- Panic buttons to raise an alarm
- Sensors adjudicating if the bus was getting rightly parked on any bus stand (keeping a log of the each no. of parking, while also helping the driver to park at every bus station on daily route)
- Cameras to manage the Bus stands (passengers vs miscreants)
- GPS for tracking the bus location and their respective timings

Management of the overall eco-system

- Vehicle dispatch & scheduling system
- Bus terminal management system (BMS + Physical Security)
- RFID for the busses and their respective terminal for allowing only the accredited buses.
- Special security governance for the bus crew.
- GPS based fleet monitoring system
- Incident management system reflecting all SLAs and sub SLAs
- Business Intelligence systems to improve business and productivity

<u>Management of the overall eco-system</u>

1. The buses in each of the depots have to be grouped into few no's, so that the buses can go through scheduled maintenance & repair work and be ready for the duties when asked for.
2. The bus terminals should be secured since so many lives get associated, when the buses are doing its daily duties. A simple and easy technology with some stringent processes can transform an ordinary bus depot/terminal into a substantial secured zone. An access control system shall be provisioned while entering the bus terminal/depot, Access control on the bus door integrated with GPS clock. Futuristic plan would be ignition of the bus with the right access control id.

All the repair works and maintenance work (except for some unavoidable circumstances) to be built in-house to ensure more buses availability.

3. Left side of each bus and front side of each bus stand shall have sensors to see if the bus entered and parked appropriately in the bus stand. Drawing a rectangle and a cross in its middle on the road, in front of the bus stand would further help the driver to align.

4. The entire fleet of the buses from each bus depot would be mapped on GPS and tagged for routes. Each route would be mapped as a service and would have SLA's binding them. Deviations would be instantly tracked. In some time with the start of the service, analysis can be done to improve various aspects of this business.

5. The analyzed database finally to be showcased in the Command & Communications Center for various requirements, business policies and future plans

The solution should be Integratable to the extent of being called futuristic

Scope of work

The project will consist of design, development, testing, installation, commissioning, training, handholding operations, and management of facilities. This project shall be designed in a manner scalable to larger fleet size, depots and terminals including bus queue shelters.

The City Bus Intelligent Transport System shall bring a state of the art system for enhancement and monitoring of operational efficiency and automation to its transit and other allied operations. The system is expected to meet the Authority's objective of enhancing service standards, better planning and efficient operations; bring in commuter centric services, integration of para-transit, and automation of collection and payment of transit fares, revenue generation services like advertisement system.

the system will deliver the stakeholder requirements by integrating various solutions and technologies onto an integrated platform which will comprise of following distinctive application areas:

S. No.	System	Sub-System
1.	**Vehicle Tracking System**	A. Vehicle Location System
		B. Passenger Information System
		C. GIS information System
2.	**Operation & Management System**	A. Schedule Management System
		B. Integrated Depot Management with crew allocation and allied services
		C. Business Analytics Module
		D. Infrastructure Management System
		E. Fleet Diagnostic communication and management System (Vehicle Health Monitoring.
		F. Advertisement publishing and management system
3.	**Communication System**	A. EPABX integration System
		B. Crew Communication System
		C. Advertisement and Public Announcement System
4.	**Command & Communications Centre management System**	A. Integrated Command centre Management with duty allocation and allied services
		B. Web based GIS map editing and GIS Map server management system
		C. Display management system

		D. E-mail server, voice and SMS application and management system

The standards for above should (a) at least comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards.

Architecture of the system

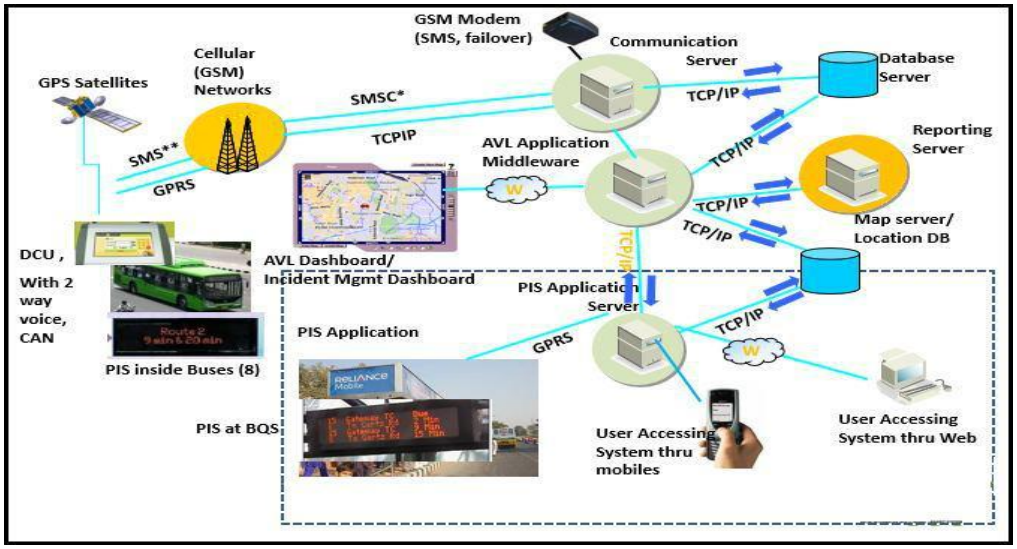
The architecture defines the overall inter connectivity of different sub systems including inside vehicle, communication within sub system and connectivity to backend solutions for the transmission of the real time vehicle information. The functional aspect of the systems and sub-systems are described as under:

1. Vehicle Tracking System

The Track & Trace Communication system will track & trace the location of vehicle running. The GPS based Automatic Vehicle Location System will be used for tracking and tracing the vehicle. The following systems are used for Track & Trace system:

a. Vehicle Location System & Passenger Information System

The Vehicle Location System gives an agency the ability to track, record, and analyze how vehicles are performing in real time. These features lead to improvements in public transit service through better on-time performance and quicker response time to emergencies. The Location information along with other details such as the speed of the bus, the route followed etc. is used to provide the passengers waiting at the bus stops with the expected arrival time of the bus. The information are displayed on boards installed at the bus stops as well as inside the buses using the Public Information System boards , announcement systems, websites, mobile apps etc. The system also helps in improving the efficiency of bus operation by generating various standard and exception reports.



Conceptual Schematic of GPS based Vehicle Location System & Public Information System (PIS)

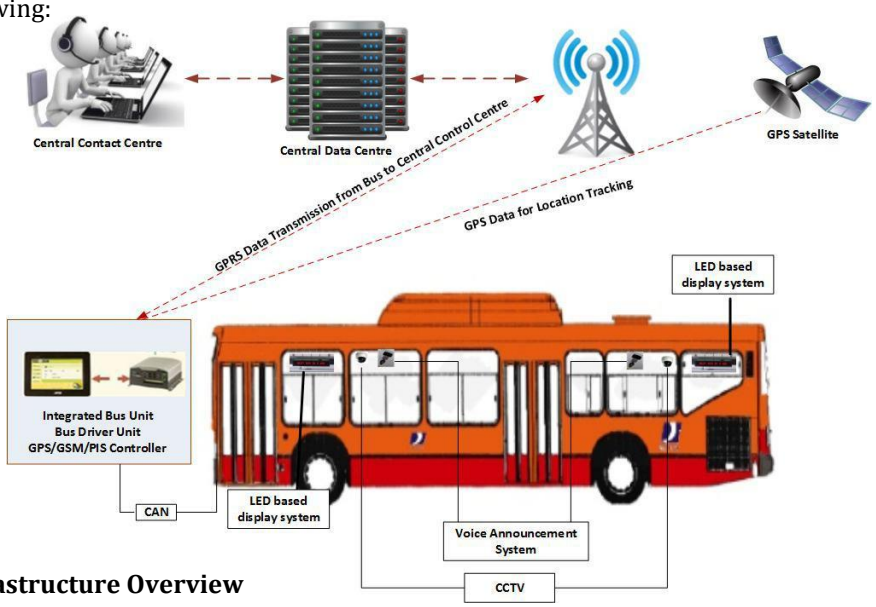
As shown in the figure above the Vehicle Location system consists of Bus Control Unit mounted on the buses which is used to send location as well as speed data to the central system for tracking the buses. The detail specification of bus mounted units shall be as per Urban Bus Specification II of MoUD, GoI. The

Bus Control Unit provides the Location data to the Communication server as part of the Central Control Centre infrastructure which processes the information and saves the data in Database server to be stored and processed for other facilities by Vehicle.

Location System application which displays this information on GIS maps and also provides the location, speed and route data to the Estimated Time for Arrival (ETA) application to generated ETA for various bus stops. The Vehicle Location system will facilitate the Passenger Information System (PIS) to disseminated this ETA information to commuters in various modes like display screens, voice based information on buses and stop/station, web portal, mobile information delivery system, SMS based enquiry system.

b. On-Board System

The GPS/GPRS based bus control unit is an integrated control unit which will control the in bus display boards as well as the announcement system. A bus may have up to four display boards mounted inside to display the upcoming Bus Stop & other relevant information. The ITS system planned for bus operations include following:



Bus ITS Infrastructure Overview

a) ITS at Bus Stop/Station/BQS/Depot /Terminals

As passengers arrive at the bus station/Stop/Depot/BQS, they need information at different stages before their departure. With bus station PIS system, passengers can easily view bus arrivals and departures as well as schedule changes, service advisories, etc. Supply of such GPRS/SMS based PIS system will be in scope of work of the bidder.. PIS system will be as below:

- PIS Display on Bus Stations
- PIS at bus stations will be connected through mobile communication to Central Control Centre GIS module to generate the ETA information for various bus stops.
- Web Portal for Bus Schedule & ETA/Mobile Application

The vender will develop integrated PIS system for web portal, Android and IOS and other leading mobile OS. This Application will have provision for advertisement. The vendor must develop advertisement publishing and management system.

c. PIS at Depot cum Terminal and Bus Queue Shelter (BQS)

LED based Passenger Information Displays (Stations will have 2 number of LED based display terminals). The PIS information will also be made available via website, SMS and mobile apps. These applications will enable commuters to be able to plan their journey well in advance and will also ensure less waiting time at the stations). Each BQS will have two number of LED based display terminals. The vendor shall be responsible for Supply, Installation and Insurance of PIS. All spares required for the smooth operation of the ITS system shall be maintained by the vendor for the entire duration of the contract.

2. Centralized control centre

One Central Control System at state level will generate the necessary management reports received from the GPS based Vehicle Tracking system and PIS. The Central control center will monitor the movement of vehicles to ensure their adherence to speed limits, routes and punctuality. Central control center will overall monitor and support entire operation like user creation, online support, Depot control centre/other control centre management and Data centre operation etc.

The vendor shall develop application module for the smooth operation of Central control center, and shall deploy support and maintenance manpower at the central/depot control center.

3. Operations Management System

The operations management system for the city bus will consists of the following system modules in integrated mode with the all other application system module. Basic functional requirement are as follows:

a. Scheduling Management System

The Schedule Management System will provide city bus operator the ability to react quickly to operational problems such as:

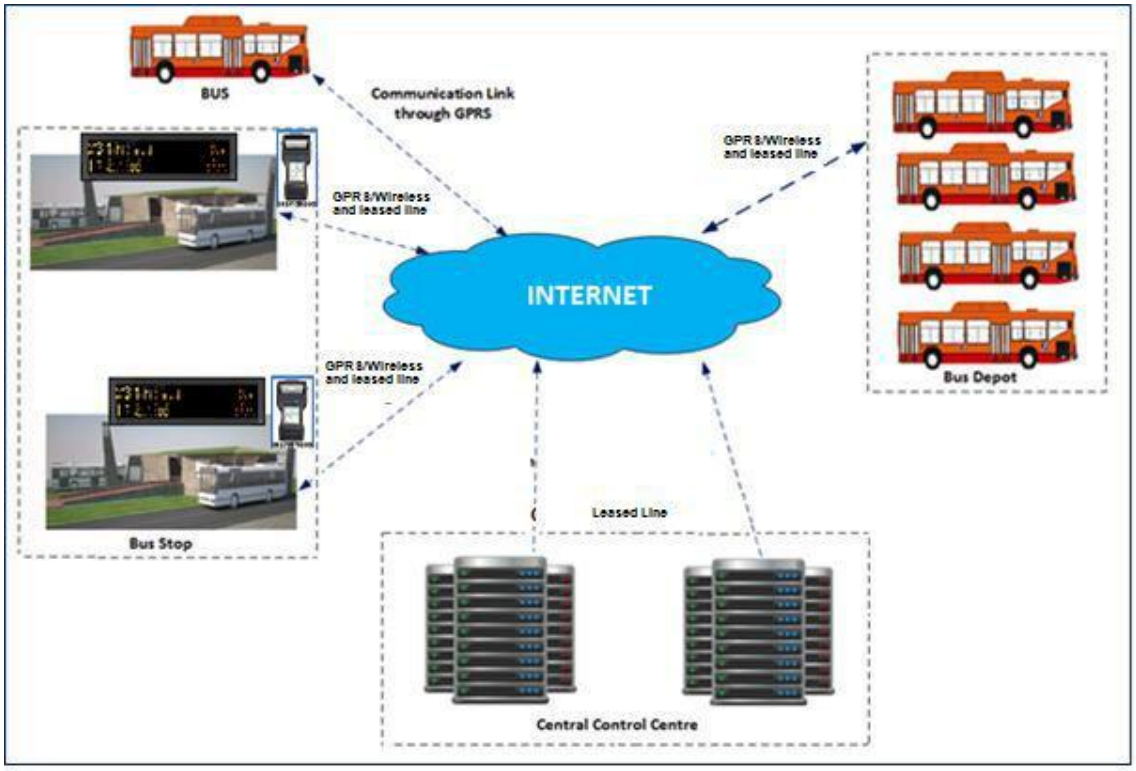
- Provide daily Fleet Service Schedule, Maintenance Schedule, pending Insurance and pending Pollution Check status
- Vehicle job cards are prepared based on complaints and scheduled service
- Define schedule of duties in various routes.
- Creation of Conductors and Drivers Duty Roster.
- Allows sending a vehicle in exchange of brake down/detained vehicles.
- Records fuel taken in by each vehicle and provides average fuel consumed per kilometer. Automatic updation of changed Time Table in the Duty Roaster.
- Record each vehicle's scheduled and actual out time from bus stand and depot and scheduled and actual entry time in depot using RFID as well as without RFID.
- Integrated depot management with crew allocation

Application will accomplish a series of specific tasks in the management of any or all aspects relating to a fleet of vehicles. Software, depending on its capabilities, allows functions such as driver and vehicle profiling, trip profiling, vehicle efficiency, etc.

4. Communication Overview

The figure below shows a pictorial representation of the communication network plan for city bus system. The communication system design is a very important part of the overall system design as the appropriateness of such design will influence the sustainability and operability of the system as a whole.

The communication network depicted above takes in account the operations requirement as far as bus, bus station, depots, terminal's, data centre, control centre and data recovery site is concerned.



General Packet Radio Service (GPRS)

GPRS is required to be used for services such as Wireless Application Protocol (WAP) access, Short Message Service (SMS), Multimedia Messaging Service (MMS), and for Internet communication services such as email and World Wide Web access.

The information captured by the Bus Control unit is to be transmitted to the control station server through GPRS/GSM network creating a communication network between Bus drivers, Bus stops along the road route, and passengers through passenger information system. The communication network is connected to the internet for accessing information regarding bus arrival, routes etc.

A. Overall basic system functional & operational requirement

The bidder will study the complete system including infrastructure, Buses, communications network availability etc. before bidding. The bidder through the study shall get a proper understanding of all aspect of project requirement-which might or might not be detailed in this document or may be added/amended/modified in SRS.

Track & Trace Communication System

The Track & Trace system will track & trace the location of vehicle running. The GPS based Vehicle Location System will be used for tracking and tracing the vehicle. The following systems are used for Track & Trace system. The GIS maps and map server will be developed by the vendor.

GPS BASED AVLS & PIS

A	**General Requirement**
i.	GPS based Vehicle Location System will provide the following features:
	a. Ability to locate a bus at a given time in its track to estimate its arrival/departure time at the next destination, based on traffic density, distance, speed, bus occupancy, run-time information from the previous bus arrival time for the same location etc.; b. Ability to receive SOS and alerts from moving / stranded buses enroute c. Facility to track defined vs. actual movement of vehicles, capture deviations if any. d. Facility to view vehicle movements real-time on digital maps e. Ability to provide dynamic location specific information as the vehicle approaches bus stop/station for the benefit of passengers f. Facility to generate information such as travel time estimation, average time at bus stop, passenger traffic at different location, alerts on exceptions, and logging of the journey details of the bus for each trip g. Facility for citizens to access and view position / location information on GIS maps near real time through web interface with historic data displayed on maps h. Facility for providing current information location on demand i. Provide 2-way voice communication between the driver of the vehicle and the control CCC for receiving SOS and alerts from vehicle j. Facility for playing back the recorded details of the bus movement along the authorized route k. It should enable operational managers to create locations, routes, schedules Vehicle service alerts for service and maintenance

	l. Vehicle fleet summary dashboard – quick view on vehicle fleet performance m. Register a bus on unscheduled route from backend on real time basis n. Exception recording/ actions (over-speeding, off-route detection, non- stoppage at bus stops, trip cancellation) o. Display of real-time dynamic movement of buses plying on a selected route on map, with real time ETA displayed on stop points plotted on map
	The geographical position i.e. Longitude / Latitude coordinates, of each bus stop, Depot and bus station will be identified through a survey by the CBITS vendor along with details of tourist centres / points of interest / places of attraction / monuments etc. along the route, precise distances between the bus stops in each route by the CBITS vendor
	AVL system will provide these data on real time basis at pre-determined and configurable intervals over GPRS/wireless networks and shall support both the time mode (periodic updated based on time interval and distance mode (periodic update based on distance interval)
	Transmission of Data on GPRS (primary mode of transmission), SMS (used as back-up).
	Facility to configure parameters over the air (should be supported over GPRS/SMS). These parameters include APN, Server IP or Fully Qualified Domain Name and port, Data Update frequency. Domain name registration service will be provided by [the Authority]
	Data update rate to server (configurable): Multiple modes to be supported (ACTIVE, NORMAL and STANDBY)
	AVL system will support dynamic trip configuration, enabling the crew / control room to activate individual trips, provide route numbers for the UP or DOWN trips.
B	**Operational Requirement**
	The web-based system will be capable of data communication with all the system components in real-time.
	Uploaded data will not be deleted from device readers or workstations until the central system has provided confirmation acknowledgement that the transactions have been successfully received.
	The web-based system will able to update its date and time using time synchronization application of servers. Also the date and time on all system devices and workstations should also be updated.
	The CBITS vendor will manage all device activity including data storage and processing.
	All active equipment will have an internally maintained date and time clock that is synchronized using a time interval via the communications medium with the system date and time clock.
	The systems will be driven by configurable parameters and should provide the flexibility for maximum configuration. The configurations will be for, but not limited to: ▪ Time based messages/reports ▪ User groups and users privileges ▪ Addition & deletion of equipment's, nodes, stations, user groups, users

	▪ Configurable messages in minimum English and Hindi languages ▪ Reports access
	The system will handle all degraded conditions which can be, but not limited to the following: ▪ Any supplied equipment not functional ▪ Power failures ▪ Data connection lost ▪ Central server down ▪ Bus-station switch non-functional
C	**Software location playback**
	The vendor will provide all software and hardware that comprise the overall central system, including the required number of licenses for all users.
	The software will provide controls to view the entire sequence of reported locations from the beginning of the time period or to step through the sequence incrementally forwards or backwards.
	The software will be accessed on workstations and control centers of all user identified by [the Authority]. All communications and AVL data will be stored in a manner that allows direct access by the software for at least 120 days and reporting data for 18 months live in the system. CBITS vendor will provide Utilities to support archive and restore functions for older data.
	The system will allow replay for a single vehicle, selected set of vehicles or all vehicles or cluster wise vehicle or route wise vehicle or UPTS?? wise vehicle on the selected map view for selected time period.
	The system will allow selection of any time period for the historical data. All data will be the property of [the Authority] and will be immediately available to [the Authority].
	The replay data will include location and headway adherence data.
	All users accessing the AVL software will be able to access the playback function.
	The system will allow the ability to use playback without exiting from the current AVL operational view.
	The system will be able to store a playback in a format that can be exported for viewing on any computer.
	All servers will be fully redundant and capable of automatic failover without administrator intervention.
D	**Graphical Interface**
	The central system shall be delivered with a fully functioning Graphical User Interface (GUI)
	The Graphical User Interface shall be based on standard web based browser controls or an equivalent system.

	The system will only be accessible by authorized persons, controlled using login and password protection. The login and password will be a single system for entire CBITS modules.
	It will be possible to create different user classes/categories/roles with different access level.
	The system will maintain a transaction log that records all users that access system reports. The pages/reports accessed, edits and changes to the database and the system logon and logoff times. The transaction log will maintain this information for a minimum of one year.
	The system security will provide features to maintain data integrity, including error checking, error monitoring, error handling and encryption.
	Features will be provided to ensure that all system-created files are uniquely identified, and that no files are lost or missed during data transfer.
	System will have verification features to confirm that there have been no losses of data at any point in the transfers.
	System needs to be tamper proof and CBITS vendor would build features to confirm that there have been no unauthorized changes to, or destruction of, data.
	Features will be provided to automatically detect, correct and prevent the propagation of invalid or erroneous data throughout the system.
	All systems, sub-systems and devices will only allow access to authorized user classes.
	All security breach detections will be confidential, and accessible only to users of the appropriate class.
	For all data transactions, the system security will include authentication features to verify that all claimed source, recipient or user identities are correct and valid. All data transactions will include non-repudiation features to verify message content, and resolve claims that data was not correctly originated or received by a certain user.
E.	**Maintenance Mode-Operational Requirement**
	The web-based system and all the equipment (on-board equipment, PIS displays in stations etc.) will all support a maintenance mode during repair, replacement and testing of equipment.
	All the functions that are carried out in the maintenance mode will be reported separately similar to exception transactions
	The maintenance mode will be possible to be activated based on a particular node wise.
	The maintenance mode can be activated only by a person having the highest user privilege in terms of system operations.

	Logins and logouts will be transmitted to the system, along with associated Date/Time, employee ID, equipment ID etc.
	It will be possible to upgrade the firmware/ software from the central server using the internet communication available at the station level.
F.	**Scalability/Future Operational Requirement**
	The central software will be scalable to accommodate for buses, bus-station/BQS/terminal PIS, without any modifications to the central software except minor configuration changes, the details of how scalable the system is will be provided in the proposal by the CBITS vendor at the time of SRS. The minimum scalability will be for 2000Buses, 2000 PIS for BQS and Bus terminal, 50 bus depots and 30 UPTS. Authority will not pay any excess fees for increase in volume up to scalability.
	The software will provide standard reports based on the AVL data. CBITS vendor will provide details in their proposal related to reports that are offered and the degree to which they can be configured (at minimum all report will be configurable for a specified date/time range and route). Some of the expected standard reports are as follows: a Headway adherence b Active fleet (weekday and weekend) c Service hours and mileage d Schedule Adherence e Speed Reports f Route Deviation reports
	The CBITS vendor will facilitate the UCC to generate all the reports necessary to facilitate the payments to the bus operations team/contractor.
	The software will have the capability to generate reports based on exceptions as per thresholds set by the Authority/UPTS staff for various AVL components.
	The CBITS vendor will provide tools to generate ad-hoc reports on stored AVL data.
	All reports will use standard reporting tools (e.g., RDBMS or SQL or Crystal Reports etc.) and will have the ability to export data into file formats that can be exported to and edited with standard tool i.e. excel, etc. The CBITS vendor shall provide the relational database layout including related fields, key fields and definitions for all fields in all tables in the database.
	Any portion of the transactional database will be exportable in standard formats (such as comma separated variable (.CSV, xls, xlsx files etc.) for analysis in third party programs.
	It will be possible for users to build custom reports from the data in the transactional database with tools such as RDBMS or SQL. The reports will be capable to be exported to pdf, xls, xlsx formats easily.

	A data dictionary will be provided to Authority to facilitate development of custom reports.
	The Central System will provide sufficient summarized and detailed data including features to generate standard report based on pre-established criteria, as well as as-required reports based on a user-definable set of search criteria.
	All reports will be generated using a query language and standard query engine that provides flexibility for future updates, and for creation of new reports.
	Reporting software will include the ability to generate graphs and charts based on criteria and format defined by the user.
	All reports will be generated with configurable time parameters, including as a minimum annual, monthly, weekly, daily, hourly and with user defined start-end date and time ranges.
	The SI will provide an ad-hoc reporting function and interface into the data and reports server to allow Authority personnel to create, execute and receive custom reports without Authority assistance with integration with fare collection system. An Internet-based interface will be provided for this function, accessible by Authority personnel with appropriate permissions. Authority users will be able to generate ad-hoc reports and do additional analysis of ridership, revenue and other System data. The SI will provide Authority's staff to generate reports and use the system. Examples of the types of reports include: • Transaction-level reports by stop and for user-defined start and end points; • Statistical and research reports using user-defined criteria
	It will be possible to aggregate data (filter) for reporting, at a minimum, by: 1. Date/Time 2. Origin 3. Destination 4. Location 5. Equipment Serial Number It will not be necessary that values be consecutive for the purposes of aggregation (e.g. non-consecutive months).
	The actual bus operational business rules will keep varying and Authority/UPTS will share the same with the SI from time to time and the vendor has to reflect it in the ITS application for generation of any additional reports etc. The cost of which will be deemed to be included in the monthly annuity cost.

G	**Web Portal and Map**
	The CBITS vendor shall develop a Modular CMS based website. The user will be able to enter in the route, direction, station/stop ID or select these from a sequence of drill down lists and from a map.
	The CBITS vendor will be responsible for the design and development of the website, including all required HTML, scripting, and integration with the AVL system. The CBITS vendor will be responsible for the integration and setup of the website. The website GUI will allow for the graphical presentation of vehicle locations on GIS-based maps.
	The AVL software will incorporate maps to support the functionality, comprised of a selection of individually selectable theme layers (e.g., stations, streets, names, water features, parks, major buildings etc.). CBITS vendor may use [the Authority] existing GIS base-map or Google map for this purpose
	The CBITS vendor will provide a GIS based base map for the purpose of the project at appropriate scale which would be acceptable to [the Authority] operationally
	The system will include mechanisms to allow for 6 monthly updates by [the Authority] to the central software maps during the contract period
	Develop additional overlay map layers to the external source map that can include polygons (e.g., municipal boundaries, fare zones), lines (e.g., route traces) and points (e.g., landmarks, transfer locations, time-points, stops), with the color, shape and thickness being selectable.
	The software will allow users to view the map, including a selectable combination of the source map layers and new layers, at various user-defined zoom levels.
	The map display icon for each vehicle location to display as the label the vehicle, block or route.
	The display icon of the bus on the map will provide an indication if the latest reported location being displayed is older than the reporting interval or not, to identify packet losses and delay in communication transfer.
	The system will track headways at corridor stations for each individual route serving the station, all routes serving the station, and for any user-specified combination of routes serving the station.
	The system will highlight to the operator the vehicle IDs of those vehicles that are operating with incorrect headway, using tabular and map displays to indicate their current headway adherence status.
	The system will provide a real-time output of the current location and schedule adherence for all fleet vehicles, for use by the next stop prediction software. The CBITS vendor will document and provide to [the Authority] the communications protocols, command sets and message formats used in this interface.
H	**Real Time PIS Requirement: Prediction Software**
	The system will use the real time location and schedule adherence data to create a continuously updated table and XML data feed of the last reported location for all vehicles and the next arrival predictions for all stations/stops.

	The system will provide this data table and XML data feed such that Authority and designated third parties have the right to perpetual and royalty-free access, for the purposes for integration with future Passenger Information System (PIS) or other public information methods and importing data into the long term database.
	The CBITS vendor will also provide a data dictionary and entity relationship diagram for the data tables and XML schema documentation. The information required by the algorithm(s) will be manually entered into a prediction support database.
	The system will allow the user to configure the prediction support database values.
	The percent error for next vehicle arrival time predictions at a given station/stop for a given minute in advance of arrival will be calculated as: absolute value of (predicted time to next arrival minus observed time to next arrival) divided by (observed time to next arrival). For example, if the observed time to next arrival was 7 minutes relative to a predicted time to next arrival of 8 minutes, the percent error would be 1/7 (i.e., 14%).
	The LED half-life (time until light output has diminished by 50% from the original rated value) will be a minimum of 100,000 hours
	Real time duplex communication to the PIS will be through the GPRS connection to the sign.
	The PIS will be able to display a message composed of any combination of alphanumeric character fonts and punctuation symbols. PIS will also allow both Hindi and English fonts to be displayed simultaneously.
I	**Documentation**
	The documents to be developed include: a. Site and System Survey document that shall provide the understanding of the Bidder b. Hardware Design document that shall provide the solution of the bidder c. Software Design document that shall provide the details of the software, d. including the AVL Application Software as per requirements of Authority. e. System Requirement Specification (SRS) that will detail out the CBITS vendor system design development, integration understanding and how they map with the requirements. f. Installation diagrams for all supplied equipment.
	The vendor shall develop detailed test plans that cover the requirements. Test Plans shall be developed for all components of the project, including and would need to be approved by Authority: a. Bus Control Unit (BCU) FAT b. PIS Display Board FAT c. ALL Application Testing d. Software Testing e. Hardware Testing f. System Acceptance Testing g. Operations Acceptance Testing

Hardware Requirements

A	**GPS Based Bus Control Unit (IN Built In All UBSII buses)**
	The GPS based BCU already installed on all buses.
	GPS Based BCU will update the location information like Latitude and Longitude to the central server through GPRS.
	The tracking system / GPS Based BCU fitted in the buses will calculate the positions from the GPS receiver and transfer the data to the Control Centre Server through GPRS interface for processing /prediction of arrival time of buses at different bus stops. The GPRS tracking unit fitted in the bus will also transfer the current LON/LAT data to the bus mounted display for display /audio announcement of Bus Stops.
	The GPS Based BCU with wireless communication module (based on GPRS) shall be used to provide vehicle tracking accurately and reliably. The following are minimum list of features required: a. GPS based BCU will consist of a GPS receiver with inbuilt GPS Antenna, GSM/ GPRS receiver, etc. to enable services such as vehicle tracking, communication and control in connection with a backend control centre system. b. The device is pre-installed on each City Bus fleet vehicle and integrated with all the other in-vehicle ITS functions and hardware being installed (e.g., Automated Stop Announcement Variable Message Signs and Public Address amplifier with speakers, Cellular Data Modem, Transit Signal Priority Emitters, Bus Door Sensors), and will support the data transfer to/from the central system through a commercial cellular data network. c. GPS Based BCU will be mounted inside the vehicle and shall be vibration & shock resistant, heat resistant, dust resistant and water / rain splash resistant and shall be tamper proof. It should as per to relevant Indian or International standards. The detail specification of BCU will as per JnNURM II i.e. http://jnnurm.nic.in/wp-content/uploads/2013/01/ Chapter-10-ITS.pdf d. The device will be operated from vehicle battery connection but will preserve battery life by tying its operation and that of the other on board equipment being installed under this contract to the bus ignition switch. e. GPS Based BCU software will be upgradeable/ configurable. CBITS vendor support team will help in such firmware upgrade.

	f. The BCU within the bus shall be easily accessible for servicing to specified vendor but located to prevent tampering or unauthorized removal. CBITS vendor must inform Authority/UPTS for such unlawful activity.

B. In Bus Display System	
	This inbuilt Bus display system will have front display board, rear display board, side display board each
	The functionality of In Bus Display System is as follows: a. PIS will be used to display information to passengers at each station along the corridor. b. The next arrival bus stop information and the current bus stop information will be displayed inside the bus for the passengers based on the location information collected by bus control unit. This information will be sent from the control unit to display system. c. The display will automatically display the bus stop name and produce audio announcement when the bus reaches a particular stop based on the signal derived from the AVL.. d. The display characteristic will be two lines English /one line Hindi language with upto 6 characters, on front, side and rear signs. e. Fixed, scrolling and flashing mode (with fixed route number, upto 6 characters, on front, side and rear signs). f. The detail specification of in bus display system will be as per JnNURM UBS II specification i.e. http://jnnurm.nic.in/wp-content/uploads/2013/01/Chapter-10-ITS.pdf
	C. Bus Terminal/Stop/Station/BQC
	Bus Stop LED Display
	The LED Display unit will display details of arrival and departure information of the buses in Hindi and English. The information of the buses such as Route Number, Bus Number, Terminal, Platform, Bay, Origin, Destination and Estimated Time of Arrival (ETA) & Estimated Time of Departure (ETD) will be displayed in both Hindi and English. The LED units should be GPRS capable with capability to configure the system remotely. The refresh timing for ETA & ETD should be 30 seconds.
	The Bus Stop display system standards requirements is as follows:

	a. Fitment provision will have to be provided in the Bus Stops along with necessary power supply made available. The source of power will be provided by UPTS and power bills will be paid by concern UPTS. The Display Unit will source power from here for its operation. Display will be located at a convenient height to have a clear view of the message of next arrival bus. b. The Bus Stop Displays will periodically query the CBITS through GPRS request. c. The Control Centre, which receives the current position of all the buses from the Tracking Unit, will disseminate the data received and transfer the relevant information like the Route No, Destination of the bus and the Expected Time of Arrival at that bus stop, to the bus stop display, which has requested for the data. d. The Bus Stop Display, which receives all such information, will display continuously until the next set of data is received. e. The Destination will be displayed in two languages i.e. English, and Hindi. f. Along with the visual display, the next bus stop will also be announced in English and Hindi. g. The Bus Terminal Displays, unlike the Bus Stop Displays will be connected through wired cable with the CS.

6.12. Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Systems to be procured

- The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
- Any manufacturer and product name mentioned in the RFP should not be treated as a recommendation of the manufacturer / product.
- None of the IT / Non-IT equipment proposed by the bidder should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in this RFP, where-in the OEM will certify that the product is not end of life product & shall support for at least 66 months from the date of Bid Submission.
- Technical Proposal should be accompanied by OEM's product brochure / datasheet. Bidders should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
- All equipment, parts should be Original and New.
- The User Interface of the system should be a User Friendly Graphical User Interface (GUI).
- Critical / Core components of the system should not have any requirements to have proprietary Platforms and should conform to open standards.
- For the custom made modules, Industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented

programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. The application shall be subjected to Application security audit to ensure that the application is free from any vulnerability.

- The Successful Bidder should also propose the suitable specifications of any additional servers / other hardware, if required for the system.
- The Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60% or less, disk utilization of 75% or less).
- SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) to affect the performance / SLAs.
- All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). PSCDCL reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all requirements specified in tender documents.
- OEMs for Servers, Enterprise Storage and Wired & Wireless LAN Access Infrastructure should be placed in Gartner MQ Leaders Segment as per latest Gartner Report OR should have double digit market share as per latest IDC Report in their respective products.
- All necessary hardware, software, licenses etc. IPR will be in the name of PMC/ PSCDCL.
- Successful bidder shall make the details of new technologies, new hardware available in the market to PSCDCL. Both, PSCDCL and SI, in agreement, will take decision of new technology/ hardware implementation in case any new/ advanced technology comes up during the contract period.

7. Payment Terms & Payment Schedule

1. The request for payment shall be made to the Authority in writing, accompanied by invoices describing, as appropriate, the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.
2. Due payments shall be made promptly by the Authority, generally within sixty (60) days after submission of an invoice or request for payment by SI
3. The currency or currencies in which payments shall be made to the SI under this Contract shall be Indian Rupees (INR) only.
4. All remittance charges shall be borne by the SI.
5. In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
6. Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
7. Taxes, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

Payment Schedule

Payments to SI, after successful completion of the target milestones (including specified project deliverables), shall be made as under:

S. No.	Payment Milestone	Timelines	% Payment
1	Mobilization Advance against Performance Bank Guarantee (PBG) submission	T	10%
2	Delivery and installation of hardware/IT/Non-IT infrastructure, Software at Command Communications Center (CCC) & Pan City wide Smart Sensors, Cameras, Emergency Call Box, Public Address System, Variable Messaging Sign Boards etc.	T+150 Days	25%
3	Commissioning, training, operationalizing & Go-Live at Command Communications Center (CCC) & Pan City wide Smart Sensors, Cameras, Emergency Call Box, Public Address System, Variable Messaging Sign Boards etc.	T+210 Days	30%
4	Operations & Maintenance Phase for a period of 60 months from the date of Go-Live of the last solution.	G+60 Months	35%

Note:
T is the date of signing of contract
G is the date of Go Live of the last phase.

8. Service Level Agreements

- Service Level Agreement (SLA) shall become the part of contract between Authority and the successful bidder. SLA defines the terms of the successful bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section.
- The successful bidder has to comply with service level requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this contract i.e. during implementation phase and for a period of five (5) years. The successful bidder has to supply appropriate software/hardware/ automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.
- For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
    - "Total Time" - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.
    - "Uptime" – Time period for which the specified services/ outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime: Uptime (%) = {1-[(Downtime)/(Total time- scheduled maintenance time)]}*100
    - "Downtime"- Time period for which the specified services/ components/ outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.
    - "Scheduled Maintenance Time" - Time period for which the specified services/ components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 10 days prior approval from Authority for any such activity. The scheduled maintenance should be carried out during non-peak hours (like post mid-night, and should not be for more than 4 hours. Such planned downtime would be granted max 4 times a year.
- "Incident" - Any event / abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
- "Response Time" - Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.
- "Resolution Time" - Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

8.1. Pre-Implementation SLAs

- These SLAs shall be used to evaluate the timelines for completion of deliverables that are listed in the deliverable.
- These SLAs for completion of individual milestones listed in the implementation schedule. For delay of every week in completion & submission of the deliverable mentioned in the section of deliverables & timeline e, the selected bidder would be charged with a penalty as follows:

Delay (Weeks)	Penalty (INR)
1 week of delay for completion of scope for any smart element	0.1% of capex of respective smart element value
For every subsequent week	0.15% of capex of respective smart element value

- In case the penalties for the selected bidder reaches 10% of the capex value in the form of penalty, cumulative of penalties for all smart elements, at any point of time during the duration of pre- implementation phase, GMVC reserves the right to invoke the termination clause.

8.2. Post-Implementation SLAs

- These SLAs shall be used to evaluate the performance of the services on monthly basis.
- Penalty levied for non- performance as per SLA requirements shall be deducted through subsequent payments due from Authority or through the Performance Bank Guarantee.
- The SLA parameters shall be measured for each of the sub systems' SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools. All such required tools should be provided by the successful bidder. GMVC will have the authority to audit these tools for accuracy and reliability.
- The upper limit of penalty would be capped at 10% of the opex value for each quarter. In case the calculated penalty crosses 10% penalty of the opex value in 2 subsequent quarters, GMVC reserves the right to invoke the termination clause.

- **SLAs for street IT infrastructure such as surveillance cameras, RLVD cameras, ANPR cameras, environment sensors, weather sensors, emergency call box, public address system, and digital display boards.**

#	Uptime SLA (Monthly)	Penalty Clause
1	Uptime >= 99.5%	No Deduction
2	Uptime < 99.5%	(99.5%- Uptime %) of monthly Operational Expense for the component. For example if uptime of component is 95%, then penalty imposed will be 99%-95% i.e. 4% of operational expense.

- Uptime definition: All devices have to be working and deliver the desired results. The no. of hours that the particular device/ equipment does not work will be treated as down time. Uptime shall be calculated as Uptime (%) = {1-[(Downtime)/ (Total time- scheduled maintenance time)]}*100. For ex, if 10 nos. of Sensors for Digital display are deployed at various locations, and 2 device/ units does not work for 5 Hrs, the total non-working device hours will be 10 unit hours (and the uptime would be {1-(10/(10*90*24)}, 10 being the number of units, for 90 days on 24 hours basis.
- The penalties would be levied for every unit down time hour.
- **SLA and Penalty for Helpdesk Response and Resolution time**

#	Parameter	Penalty Clause

1	For <= 1% of the calls not getting responded in less than or equal to 60 seconds per quarter	No Deduction
2	For > 1% of the calls not getting responded in less than or equal to 60 seconds per quarter	0.5% of the monthly opex value

- **SLA for Change Requests or enhancements**

#	Parameter	Metric	Frequency	Penalty
1	Criticality of Change – **Low**	< T, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	1 % of change request value per week for the first two weeks for each occurrence, 2 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.
2	Criticality of Change – **Medium**	< T, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	1.5 % of change request value per week for the first two weeks for each occurrence, 2.5 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.
3	Criticality of Change – **High**	< T weeks, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	2 % of change request value per week for the first two weeks for each occurrence, 3 % of change request value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.

- **SLA for issue resolution**

#	Parameter	Metric	Frequency	Penalty
1	Severity 1 Issue	Resolution Time: <= 8 Hrs from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.

2	Severity 2 Issue	Resolution Time: <= 4 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.
3	Severity 3 Issue	Resolution Time: <= 10 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.
4	Severity 4 Issue	Resolution Time: <= 20 Days from the time the call is logged by end user.	Daily	0.1% of monthly opex value per week for the first two weeks for each occurrence, 0.2% of monthly opex value per week for every subsequent week, subject to a maximum of 10% post which Authority may invoke annulment of the contract.

- **Miscellaneous SLAs**

#	Parameter	Metric	Frequency	Penalty
1	Compliance in document versioning and maintenance (FRS, SRS, Business Blue Prints, User Training Manual etc.), application version control, updates & patches etc.	100% as per requirement timelines	Daily per occurrence	Rs.10,000 per occurrence per day of delay.
2	Manpower Availability & Readiness	100% as per requirement timelines	Daily	Rs 10,000 per day in case there is shortage in manpower deployment or lack of adequate skills

3	Scheduled downtime for System Maintenance per week	<= 2 times per month	Per Occurrence	Rs. 1,00,000 per occurrence for unscheduled downtime or scheduled downtimes exceeding the specified metric.
4	Resource Replacement	Within 7 days of exit of resource (in case of Authority initiated or supplier initiated)	Per Occurrence	Rs. 5,000.00 per day of unavailability of resource
5	Application Security	Cyber Crime / Hacking / Data Theft / Fraud attributable to the service provider	Per Occurrence	Depending on the type of incident and its impact, a Penalty of 10% on the entire contract value or in case of severe issue (as defined by Authority) such breach may lead to termination of contract

Definitions:

- Severity 1: Command and Communication Center or ERP or Smart City applications down for more than 70% users.
- Severity 2: Command and Communication Center or ERP or Smart City applications down for more than 30% users.
- Severity 3: Modules of Command and Communication Center or ERP not functional for users.
- Severity 4: Minor functionality issues with Command and Communication Center or ERP or Smart City applications
- Response Time: Response time is defined as the time the support vendor takes to respond from the time that ticket was raised.
- Resolution Time: Resolution time is defined as the time the vendor takes to resolve the issue or provide acceptable workaround for the issue.

8.3. Conditions for No Penalties

- Penalties shall not be levied on the Bidder in the following cases:
  - There is a force majeure event effecting the SLA which is beyond the control of the successful bidder. Force Majeure events shall be considered in line with the clause mentioned RFP.
  - The non-compliance to the SLA has been due to reasons beyond the control of the successful bidder.
  - Theft cases by default/ vandalism would not be considered as "beyond the control of bidder". Hence, the Bidder should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired Required SLA.

Annexure 1 Matrix for Scope of Work

#	Key Activities	Deliverables	CCC	Surveillance	Sensors	Emergency Call Box	Public Address System	Digital Display Boards	ERP System	Portal/ Mobile App
Project Inception Phase										
1	Project Kick Off	1. Project Development Plan 2. Risk Management and Mitigation Plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2	Deployment of manpower		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Requirement Phase										
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification Document 2. System Requirement Specification document 3. Requirements Traceability Matrix 4. Site Survey Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
4	Assessment of Business processes		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5	Assessment of requirement of Software requirements		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	Assess the Integration requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
7	Assess the connectivity requirement all locations (including Building)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8	Assessment the Network laying requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
9	Assessment of training requirement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
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	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
11	Creation of Detail Drawing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
12	Detailed Design of Smart City Solutions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
13	Development of test cases (Unit, System Integration and User Acceptance)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

14	Preparation of final bill of quantity and material	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. Test Plans 12. SoPs 13. Change management Plan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
15	SoP preparation		Yes							
Development Phase										
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	Yes			Yes			Yes	
17	Physical Infrastructure setup		Yes	Yes	Yes	Yes	Yes	Yes		
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
19	IT and Non IT Infrastructure Installation		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
20	Development, Testing and Production environment setup		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
21	Software Application customization (if any)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
22	Development of Bespoke Solution (if any)		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
23	Data Migration		Yes						Yes	
24	Integration with Third party services/application (if any)		Yes						Yes	Yes
25	Unit and User Acceptance Testing		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
26	Implementation of Solutions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
27	Preparation of User Manuals , training curriculum and training materials		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
28	Role based training(s) on the Smart City Solutions		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integration Phase										

29	SoP implementation	1. Integration Testing Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
30	Integration with GIS		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
31	Integration of solutions with Command and Control Centre			Yes	Yes	Yes	Yes	Yes	Yes	Yes
Go -Live										
32	Go Live	1. Go-Live Report	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Operation and Maintenance										
33	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	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
34	SLA and Performance Monitoring		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
35	Logging, tracking and resolution of issues.		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
36	Application enhancement		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
37	Patch & Version Updates		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
38	Helpdesk services		Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

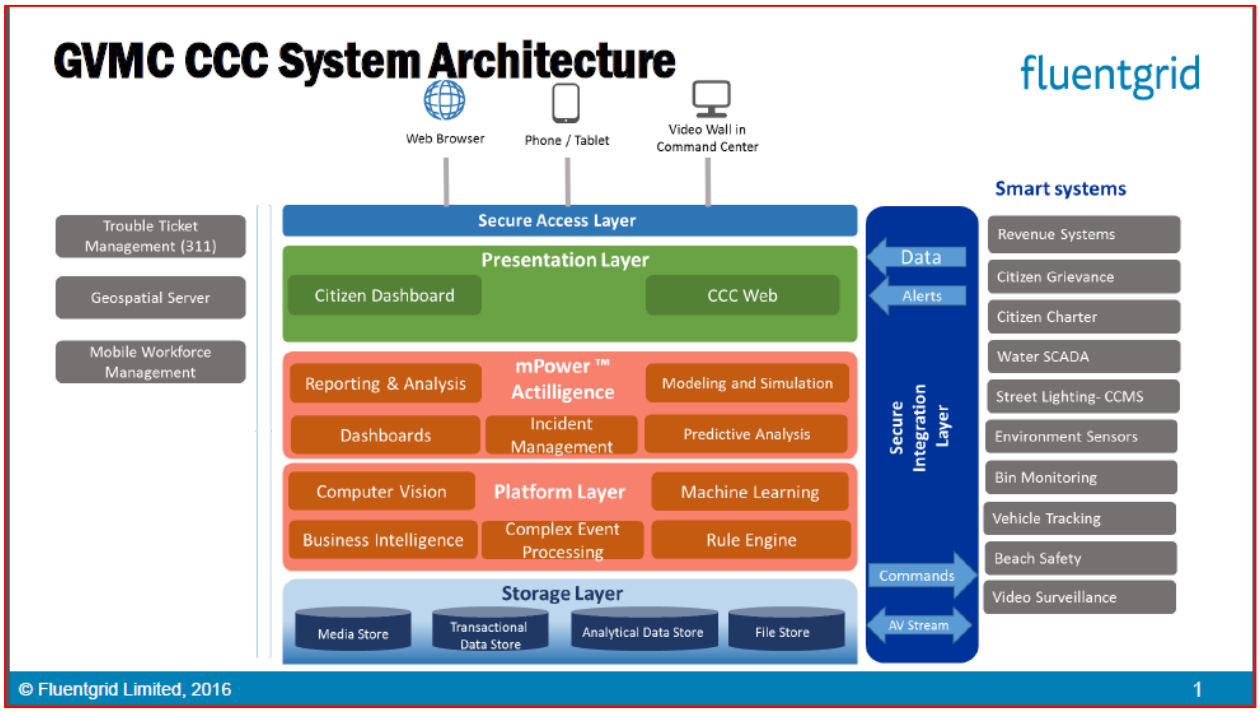
Annexure 2 – RACI (Responsible, Accountable, Consulted and Informed) Matix

#	Key Activities	Successful Bidder	GMVC	SPV for GMVC	APSFL	Electricity Providers	Other Utilities	Police	PMC	Exisitng ICT Vendors at GMVC
Project Inception Phase										
1	Project Kick Off	R/A	C	C	I	I	I	I	C	I
2	Deployment of manpower	R/A	C	C	I	I	I	I	C	I
Requirement Phase										
3	Assess the requirement of IT Infrastructure and Non IT Infrastructure	R/A	C	C	C	C	C	C	C	C
4	Assessment of Business processes	R/A	C	C	I	I	I	C	C	I
5	Assessment of requirement of Software requirements	R/A	C	C	I	I	I	C	C	I
6	Assess the Integration requirement	R/A	C	C	C	C	I	C	C	C
7	Assess the connectivity requirement all locations (including Building)	R/A	C	C	C	I	I	C	C	I
8	Assessment the Network laying requirement	C	C	C	R/A	I	I	C	C	I
9	Assessment of training requirement	R/A	C	C	I	I	I	C	C	I
Design Phase										
10	Formulation of Solution Architecture	R/A	C	C	C	I	I	C	C	I
11	Creation of Detail Drawing	R/A	C	C	C	I	I	C	C	I
12	Detailed Design of Smart City Solutions	R/A	C	C	C	I	I	C	C	I
13	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	C	C	I	I	C	C	I

14	Preparation of final bill of quantity and material	R/A	C	C	C	C	I	C	C	I
15	SoP preparation	R/A	C	C	C	C	C	C	C	I
Development Phase										
16	Helpdesk setup	R/A	C	C	I	I	I	I	C	I
17	Physical Infrastructure setup	R/A	C	C	I	I	I	I	C	I
18	Procurement of Equipment , edge devices, COTS software (if any), Licenses	R/A	C	C	I	I	I	I	C	I
19	IT and Non IT Infrastructure Installation	R/A	C	C	I	I	I	I	C	I
20	Development, Testing and Production environment setup	R/A	C	C	I	I	I	I	C	I
21	Software Application customization (if any)	R/A	C	C	I	I	I	I	C	I
22	Development of Bespoke Solution (if any)	R/A	C	C	I	I	I	I	C	I
23	Data Migration	R/A	C	C	I	I	I	I	C	I
24	Integration with Third party services/application (if any)	R/A	C	C	I	I	I	I	C	I
25	Unit and User Acceptance Testing	R/A	C	C	I	I	I	I	C	I
26	Implementation of Solutions	R/A	C	C	I	I	I	I	C	I
27	Preparation of User Manuals , training curriculum and training materials	R/A	C	C	I	I	I	I	C	I
28	Role based training(s) on the Smart City Solutions	R/A	C	C	I	I	I	I	C	I
Integration Phase										
29	SoP implementation	R/A	C	C	C	C	C	C	C	I

30	Integration with GIS	R/A	C	C	C	C	C	C	C	I
31	Integration of solutions with Command and Control Centre	R/A	C	C	C	C	C	C	C	I
Go -Live										
32	Go Live	R/A	C	C	I	I	I	I	C	I
Operation and Maintenance										
33	Operation and Maintenance of IT, Non IT infrastructure and Applications	R/A	C	C	I	I	I	I	C	I
34	SLA and Performance Monitoring	R/A	C	C	I	I	I	I	C	I
35	Logging, tracking and resolution of issues.	R/A	C	C	I	I	I	I	C	I
36	Application enhancement	R/A	C	C	I	I	I	I	C	I
37	Patch & Version Updates	R/A	C	C	I	I	I	I	C	I
38	Helpdesk services	R/A	C	C	I	I	I	I	C	I

Annexure 3 (Vizag)

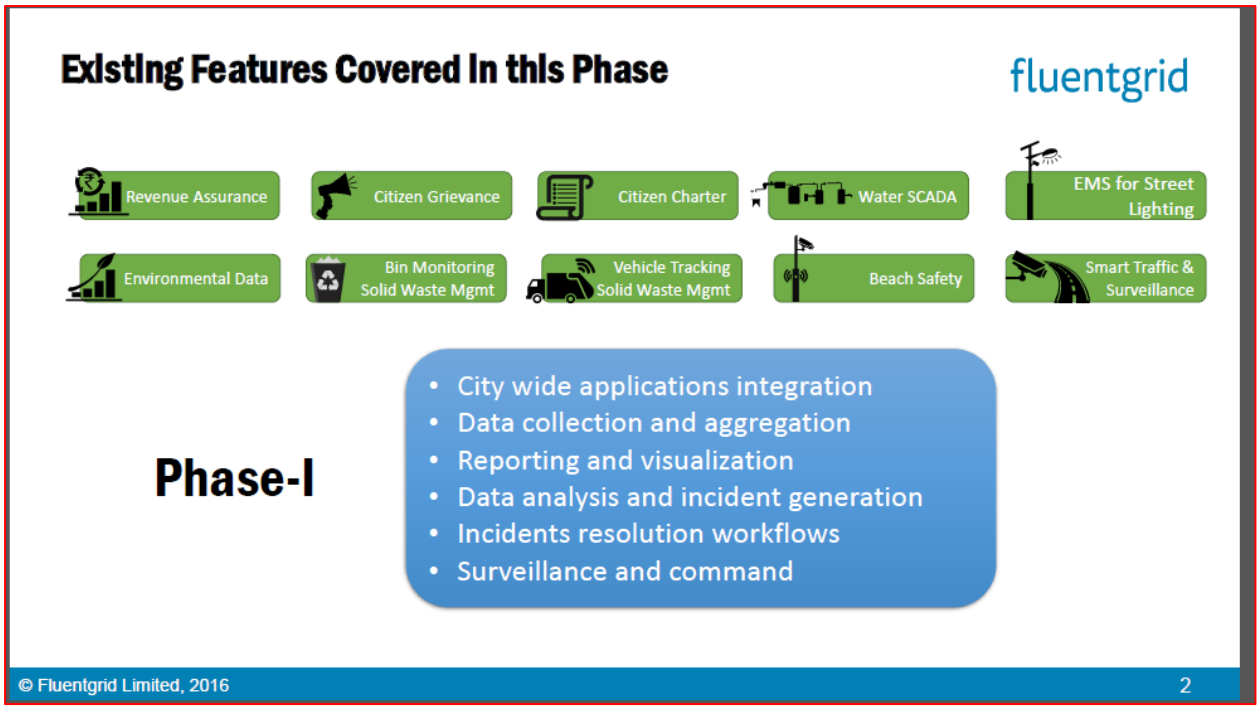


Annexure 4: Visakhapatnam Junctions list

Sr.No.	Visakhapatnam Junctions list
1.	Sea Horse
2.	Collector Office
3.	Town Kotha Road
4.	Durgalamma Temple
5.	Coastal Battery
6.	Ambedkar
7.	Dolphin
8.	Gollala Palem
9.	NTR (Beach Road)
10.	Jagadamba
11.	Watch House
12.	Turnar Chowltry
13.	Saraswathi Park
14.	Rama Krishna
15.	C.P.O
16.	Pen School
17.	Tenneti
18.	Pandimetta
19.	GVMC Gandhi Statue
20.	Taj
21.	Z.P
22.	Venkoji Palem
23.	Circuit House
24.	Patel Statue
25.	MVP Double Road
26.	VS Krishna College
27.	Asilmetta Flyover
28.	Dwaraka
29.	Siripuram
30.	Satyam
31.	Seven Hills
32.	Tycon
33.	Appugarh
34.	Park Hotel
35.	Pedawaltair
36.	AIR
37.	Sangam Sarath
38.	Sri Surya
39.	Dondaparty
40.	Rail Club
41.	Railway New Colony

42.	ICICI
43.	Gurudwara
44.	Santhipuram
45.	Akkaiahpalem
46.	Golden Jublee
47.	Tatichetlapalem
48.	Maharani Parlor
49.	A.S.R
50.	Kaprada
51.	Urvasi
52.	Muralinagar
53.	Birla
54.	Punjab Hotel
55.	R&B
56.	Kakaninagar
57.	Airport
58.	Gosala
59.	Pinagadi
60.	Convent
61.	Essar
62.	Y'' Junction
63.	Maruthi
64.	Pipe Line
65.	Cormandal
66.	Scindia
67.	Venkannapalem
68.	Karnvanipalem
69.	Gangavaram Port
70.	Kurmana Palem
71.	Vadlapudi
72.	Aganam Pudi (Hanuman Temple)
73.	Lankelapalem J.N
74.	Sheelanagar
75.	Nataiahpalem
76.	B.H.P.V
77.	Autonagar
78.	Old Gajuwaka
79.	100' Road
80.	New Gajuwaka
81.	Gajuwaka Old Traffic PS
82.	Sri Nagar
83.	Tagarapuvalasa Y-Junction
84.	Boya Palem

85.	Tagarapuvalasa Old Busstand*
86.	Car Shed
87.	Yendada
88.	Rishikonda
89.	Sagarnagar
90.	Vishalakshi Nagar NH
91.	Vishalakshi Nagar Beachroad*
92.	Jodugullapalem
93.	Hanumanthwaka
94.	Aadarsha Nagar


Existing Features Covered In this Phase
fluentgrid
Revenue Assurance
Citizen Grievance
Citizen Charter
Water SCADA
EMS for Street Lighting
Environmental Data
Bin Monitoring Solid Waste Mgmt
Vehicle Tracking Solid Waste Mgmt
Beach Safety
Smart Traffic & Surveillance
Phase-I
City wide applications integration
Data collection and aggregation
Reporting and visualization
Data analysis and incident generation
Incidents resolution workflows
Surveillance and command
© Fluentgrid Limited, 2016
2

Annexure 4: Existing Sensor Details

Sr No	System	Sensor/Endpoint Details
1	Vehicle Tracking	400 Garbage Vans
2	Street Light	5000 Switches, 1 Lakh lights
3	Water SCADA	79 Bulk Consumers
4	CCTV	423 camera (PPP model)
5	Beach Safety	1 camera
6	Weather/ Pollution	2 stations (AQ 8 parameters)